技术实战指南

Windows Server 2008



Windows Server 2008

系统安全管理实战指南

刘晓辉　李利军　编著

全新技术
案例详解
视频教学

- 案例详解Windows Server 2008安全管理新特性，涵盖系统安全平台配置、监控与管理的方方面面
- 每一主题都给出安全配置方案，让你学以致用，轻松打造安全的Windows系统
- 特别设计的具有针对性的实验课题，让你从新手快速成长为专业的系统安全管理员

清华大学出版社

最新技术·讲解全面·突出实战·轻松掌握



Windows Server 2008 系统安全管理实战指南

…光盘使用说明…

360 分钟全程多媒体实战教学

一、光盘特点

- 全程多媒体视频教学课程，完全对应本书实战教学内容。
- 动画操作演示+语音讲解+方便学习的操作界面，可让你灵活选择课程内容，自由控制学习进度。
- 高压缩Flash动画教学，容量小，播放时间长，视频教学随时加入标注解说，让你更易于理解，看得懂，学得会。

二、界面操作

- 将光盘放到光盘驱动器中，本光盘会自动播放并进入主操作界面，如果无法自动播放，可以打开光盘文件夹，找到Start.exe文件，双击该文件也可播放本光盘。

光盘主界面

Windows Server 2008系统安全管理实战指南

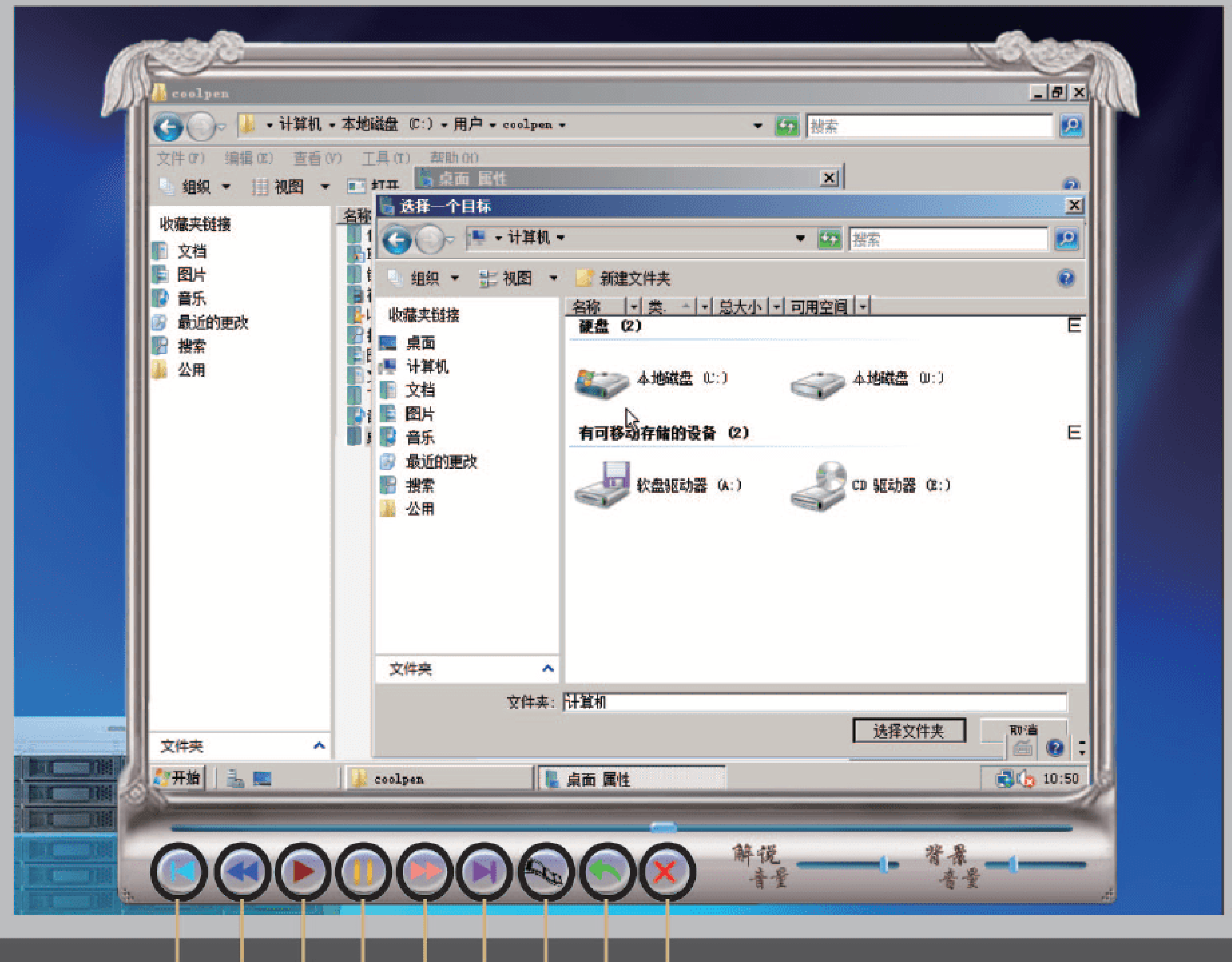
01 Windows Server 2008系统安全概述
02 Windows Server 2008环境安全设置
03 修补系统漏洞
04 活动目录安全
05 用户帐户安全
06 组策略安全
07 数据存储安全
08 文件访问安全
09 数据备份与恢复
10 电子证书和认证服务
11 系统服务安全
12 端口安全
13 审核策略与事件日志
14 Internet信息服务安全
15 Windows防火墙
16 Windows网络访问保护
17 SQL Server数据库安全

从主界面中选择要学习的课程，即可进入播放界面

帮助

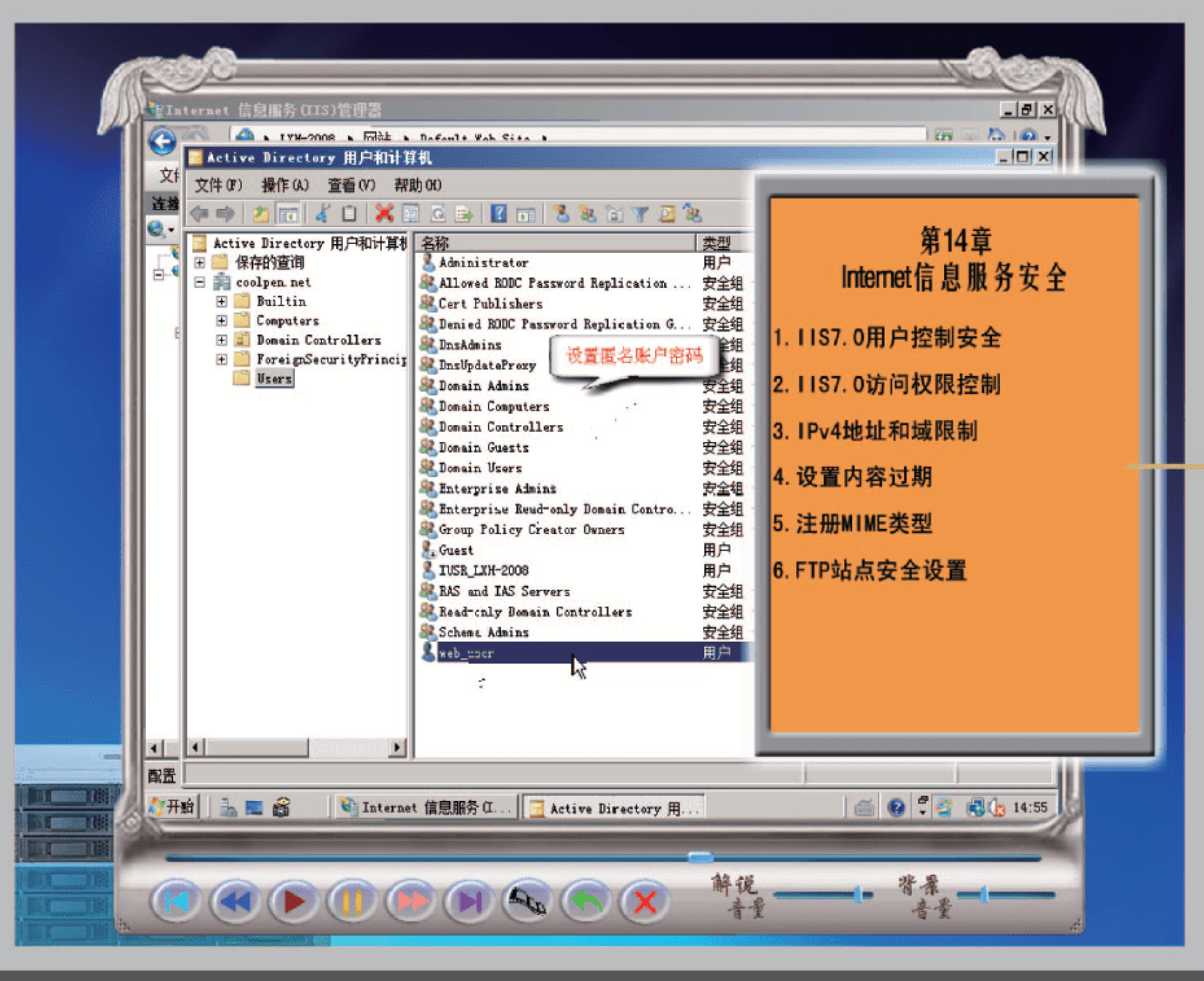
关闭

光盘播放界面



1：上一节　2：后退　3：播放　4：停止　5：前进　6：下一节　7：视频
8：返回　9：关闭

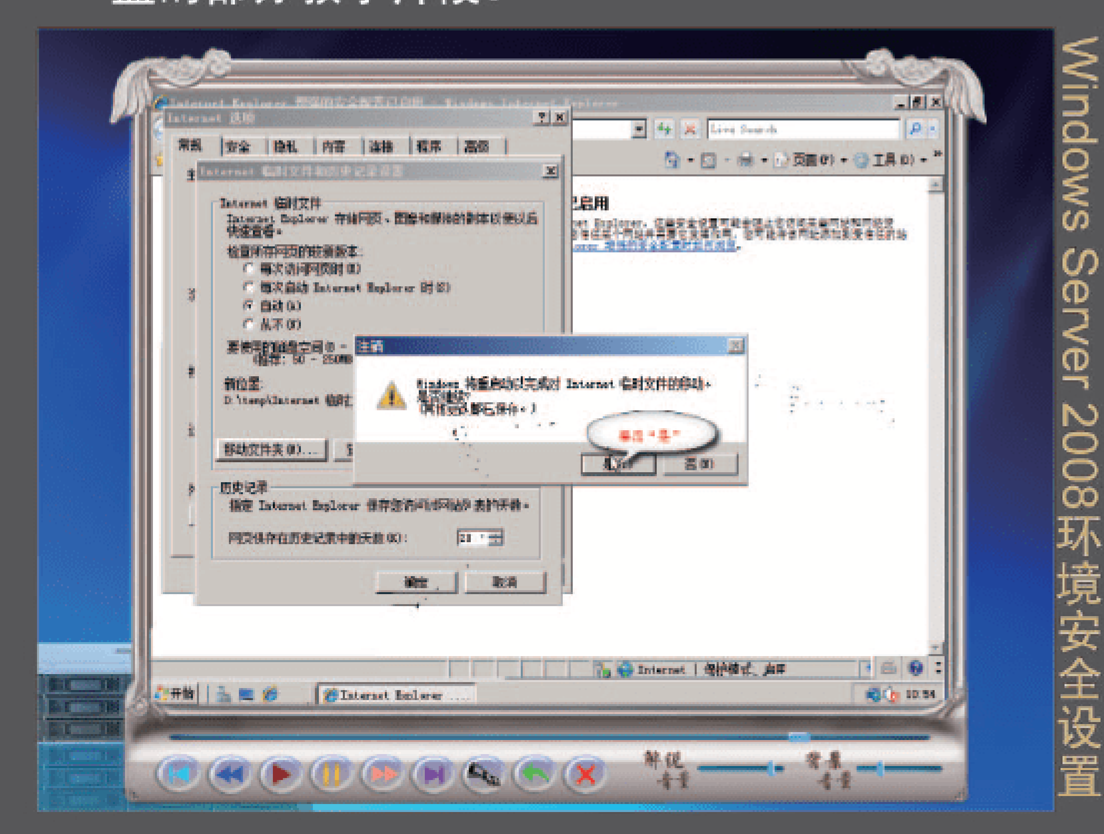
光盘播放界面



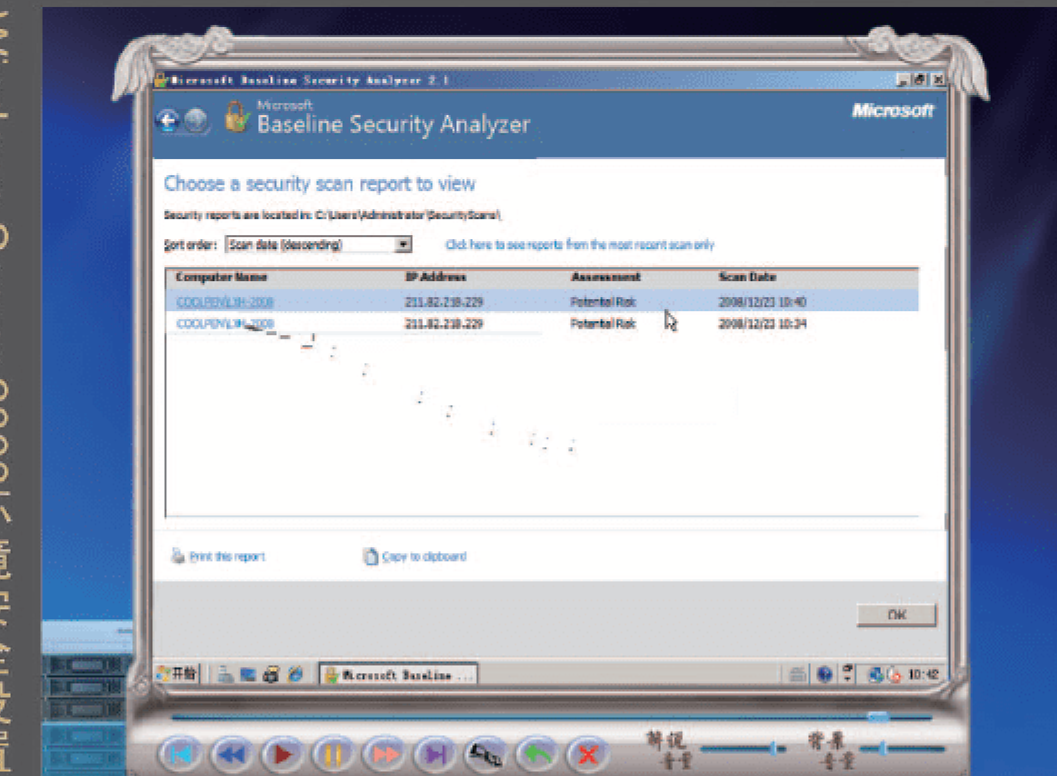
单击"视频"按钮后，打开这个视频文件选择窗口，可以从该窗口中选择要播放的视频片段

三、视频教学演示片段

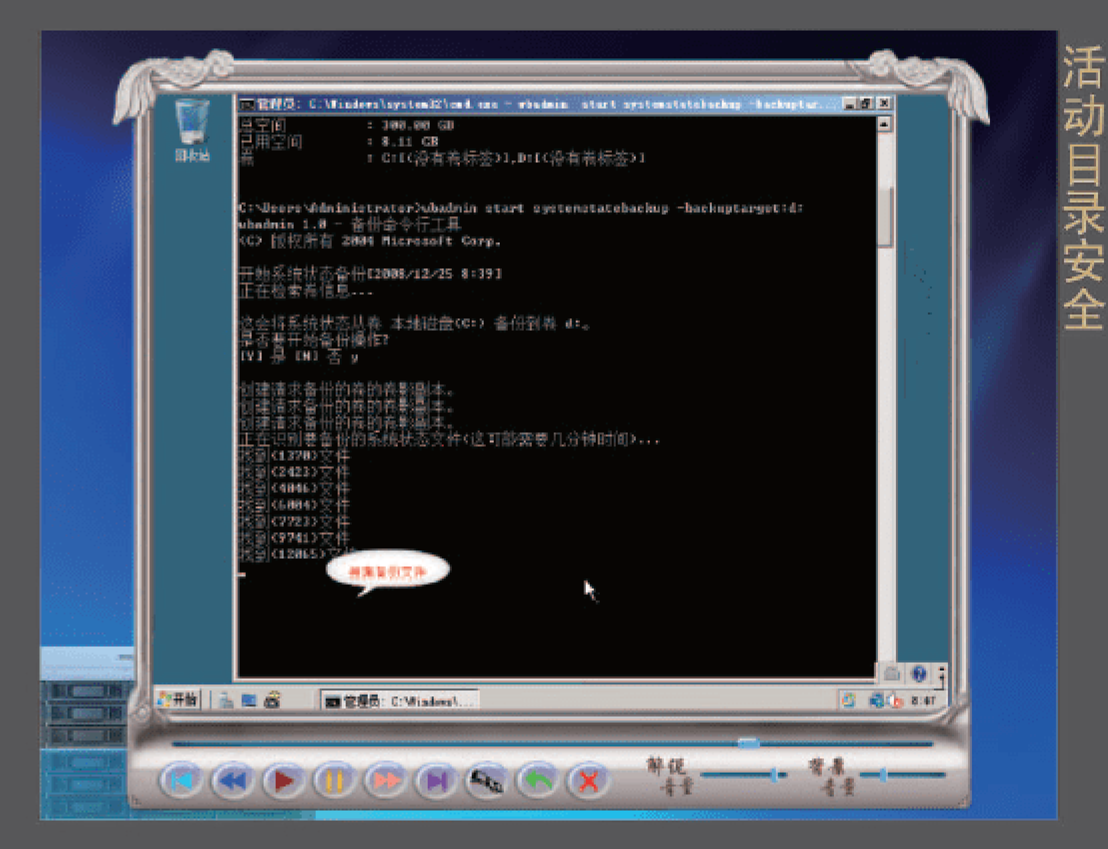
播放画面非常友好地向你演示讲解本书的各部分内容，还随时加入必要的提示文字，下面是本光盘的部分教学片段。



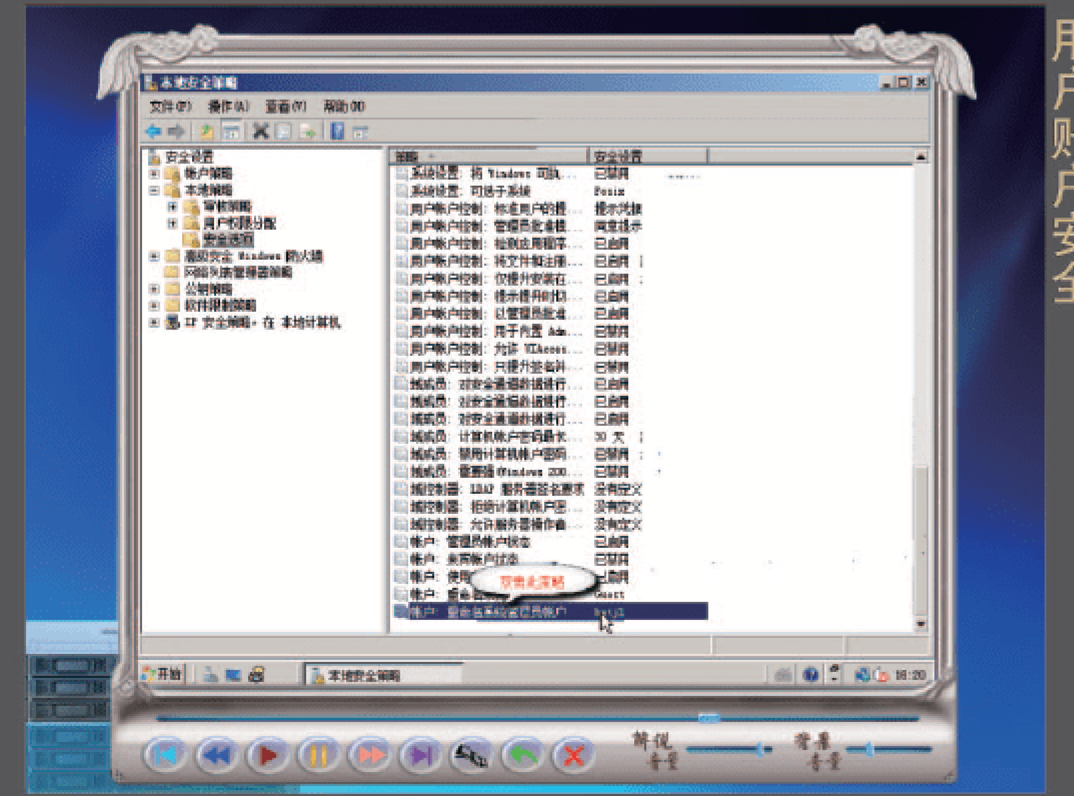
Windows Server 2008环境安全设置



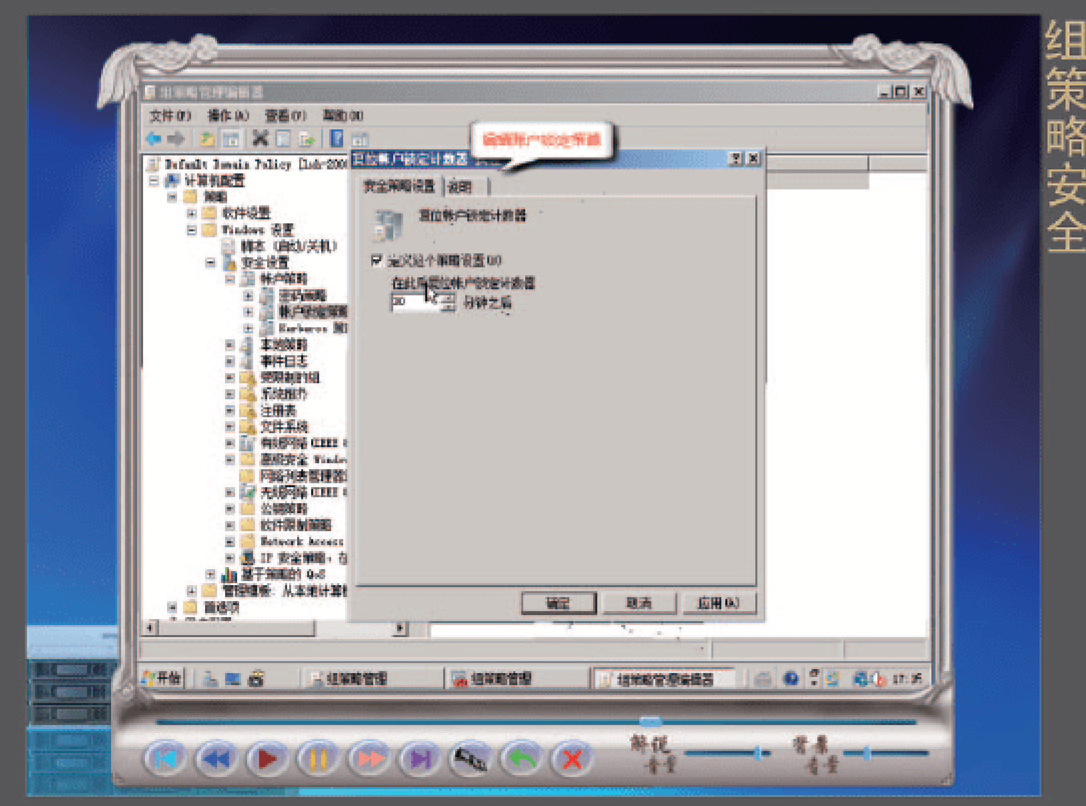
修补系统漏洞



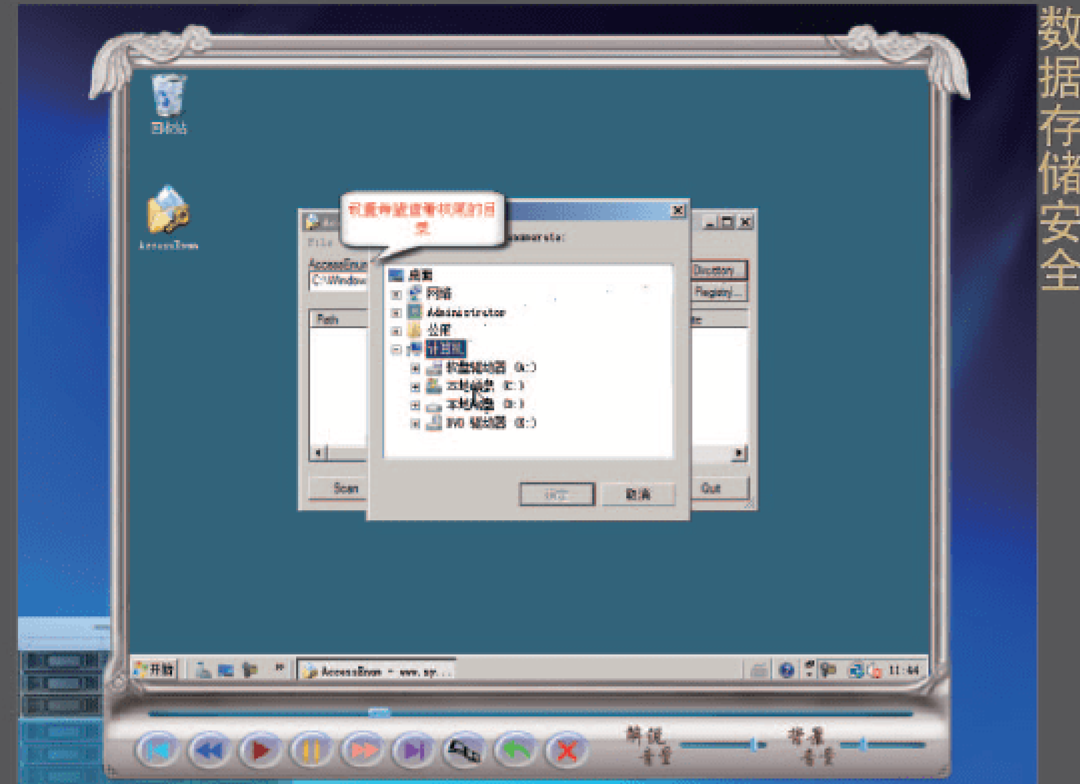
活动目录安全



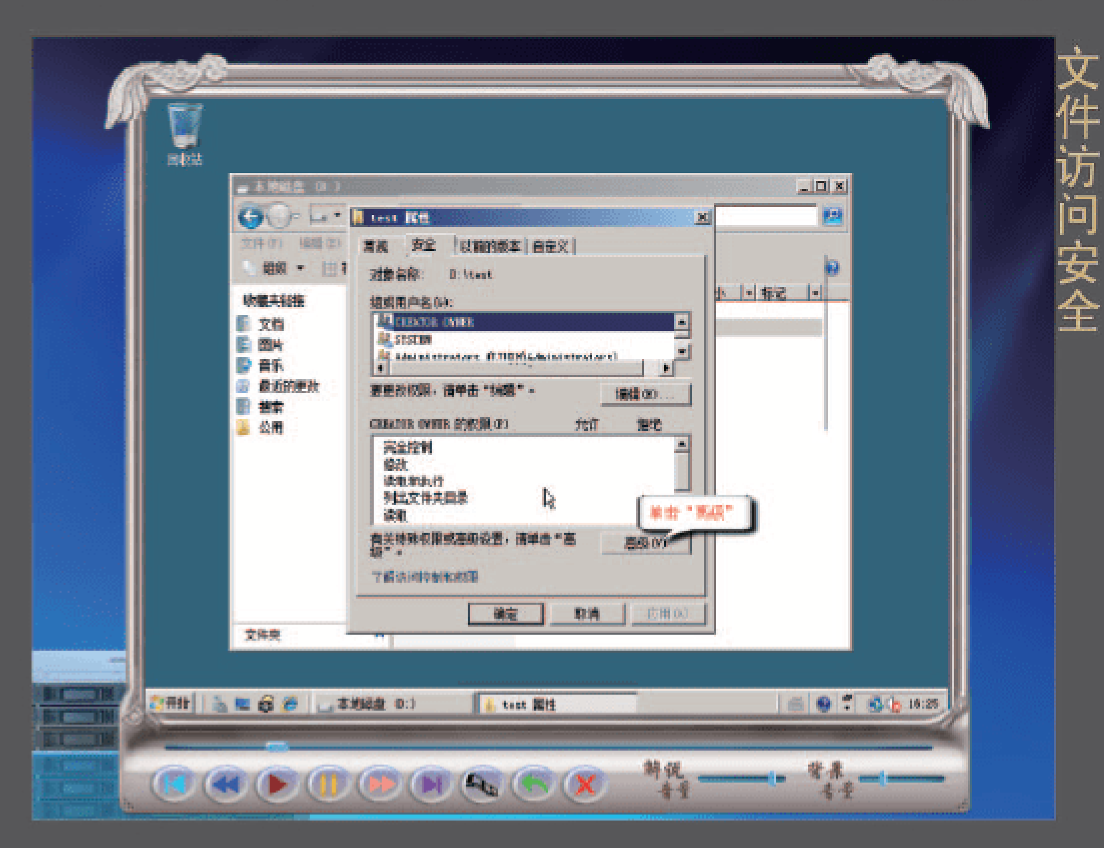
用户账户安全



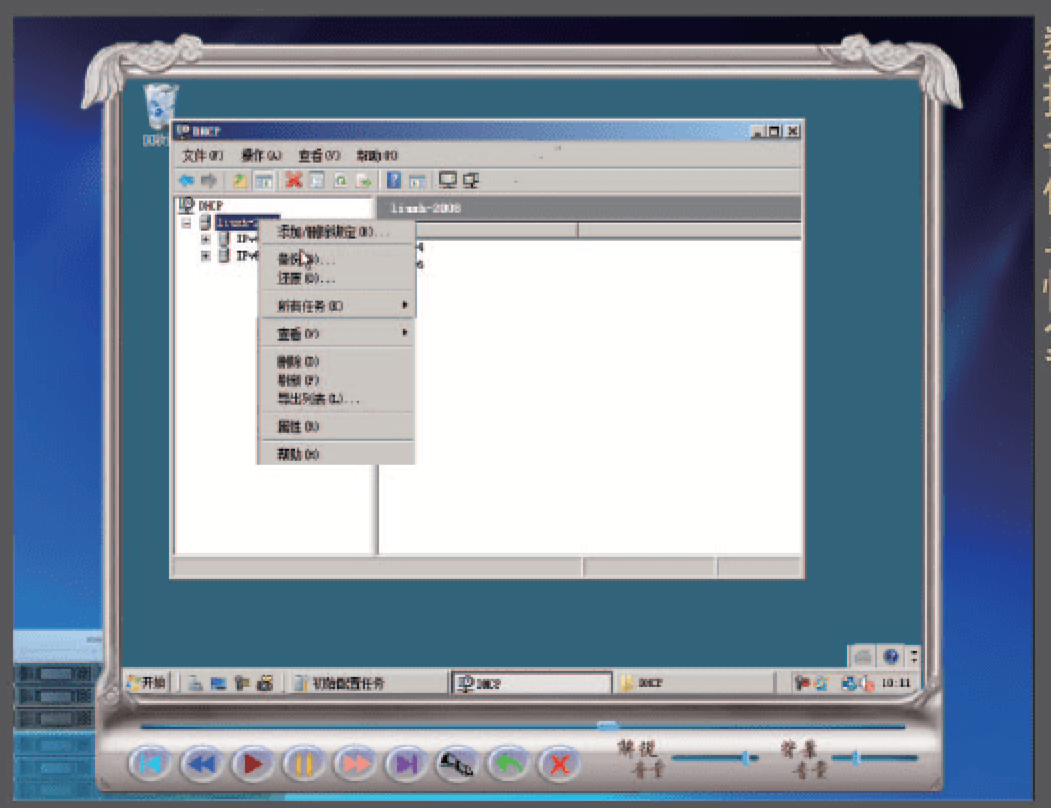
组策略安全



数据存储安全

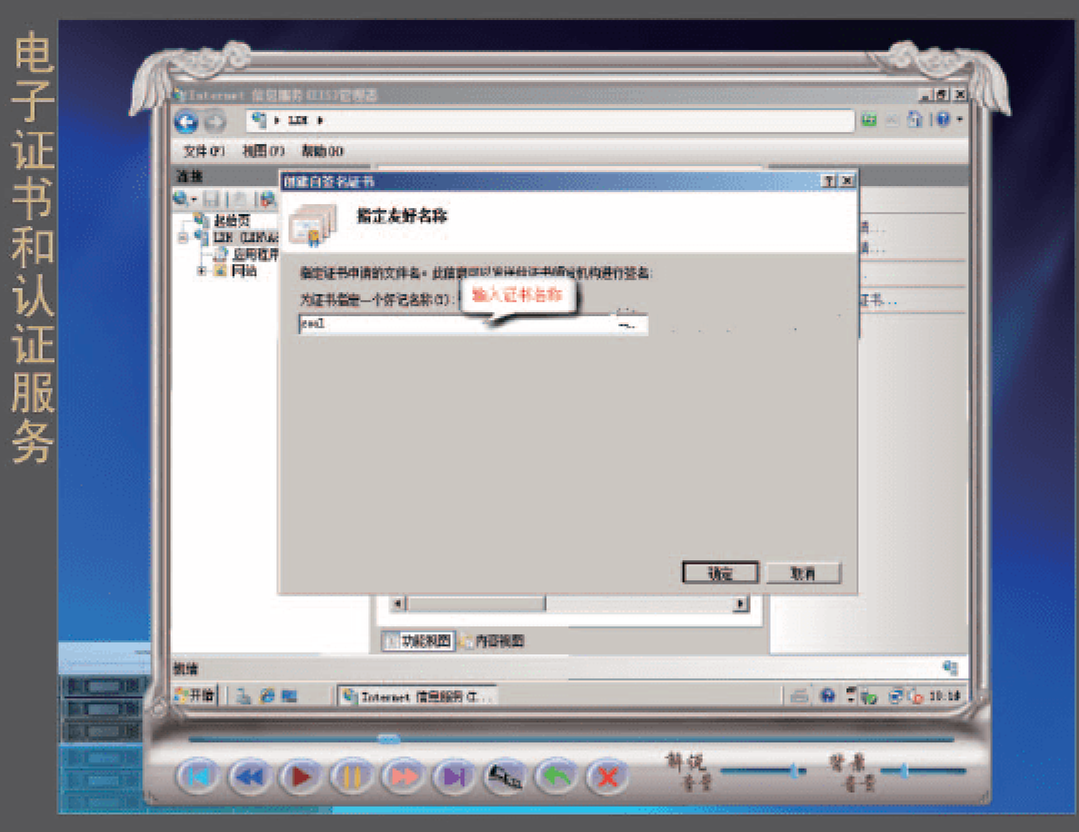


文件访问安全

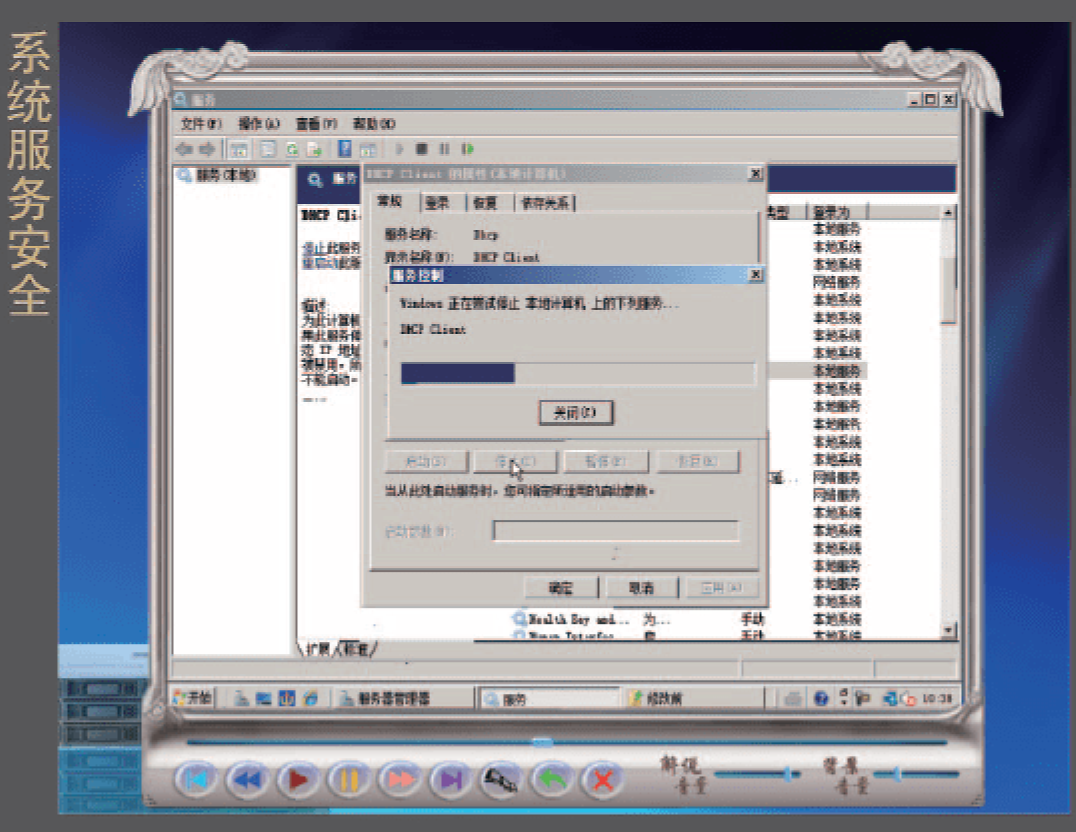


数据备份与恢复

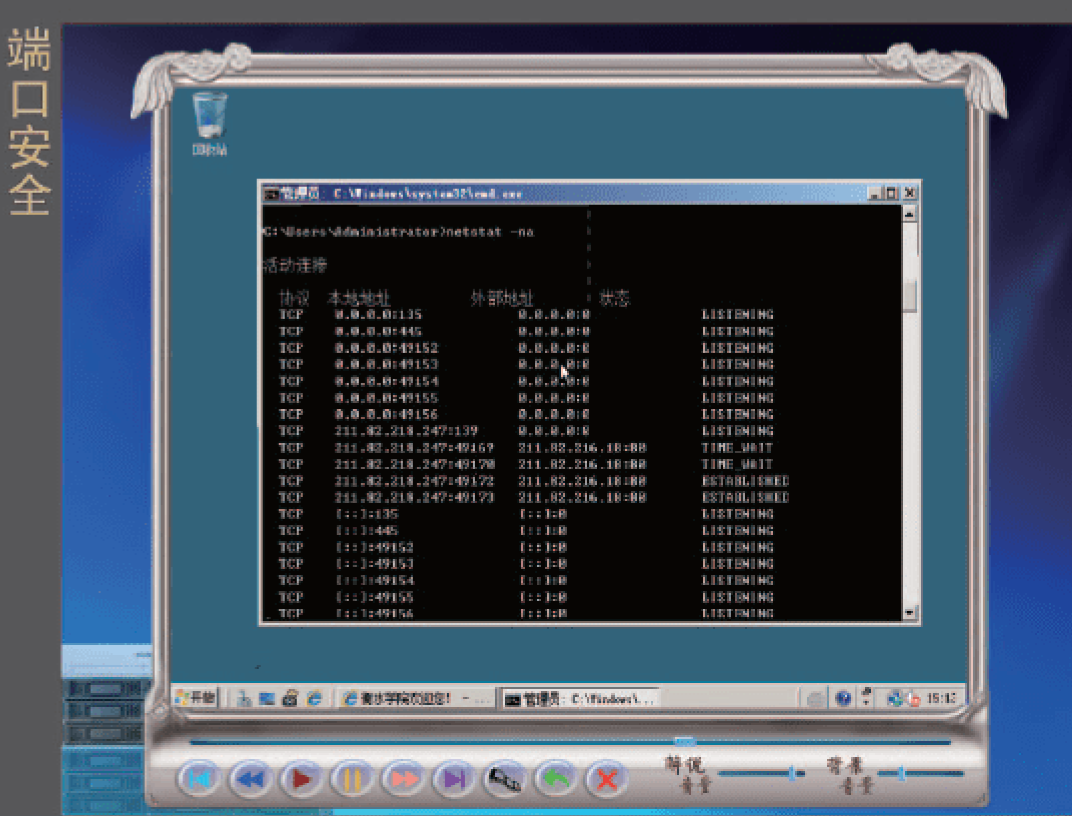
电子证书和认证服务



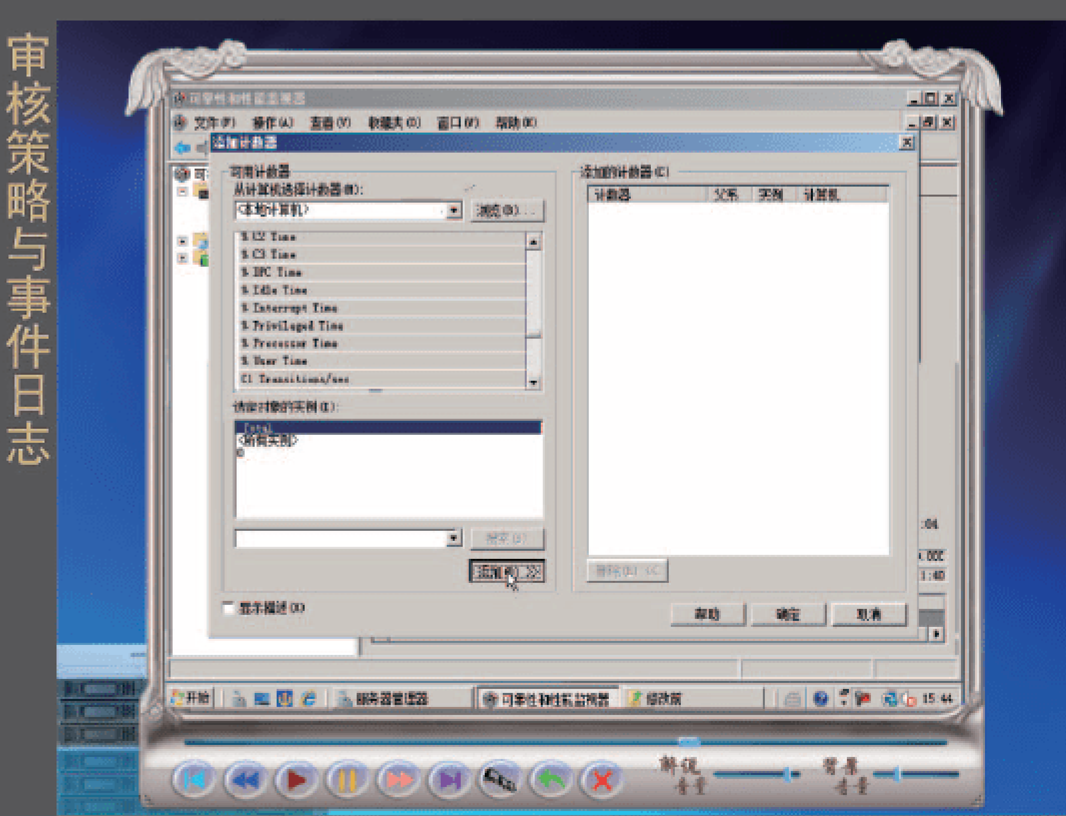
系统服务安全



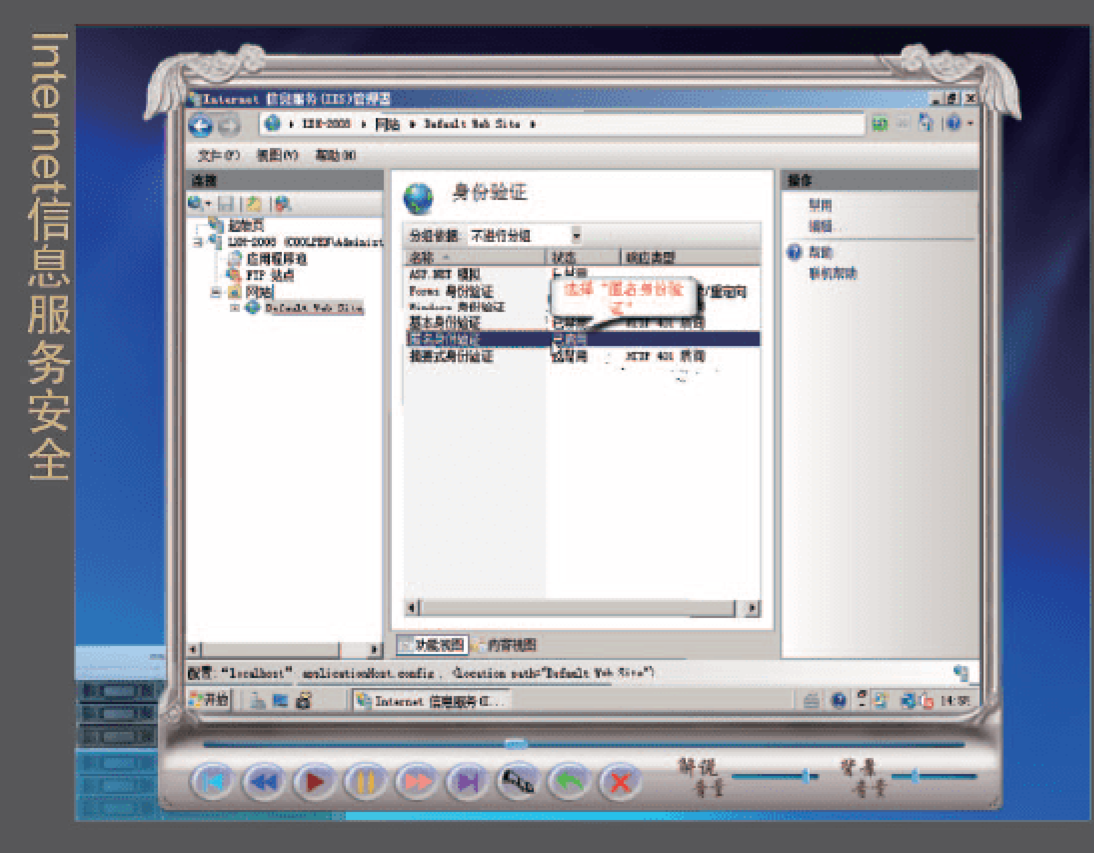
端口安全



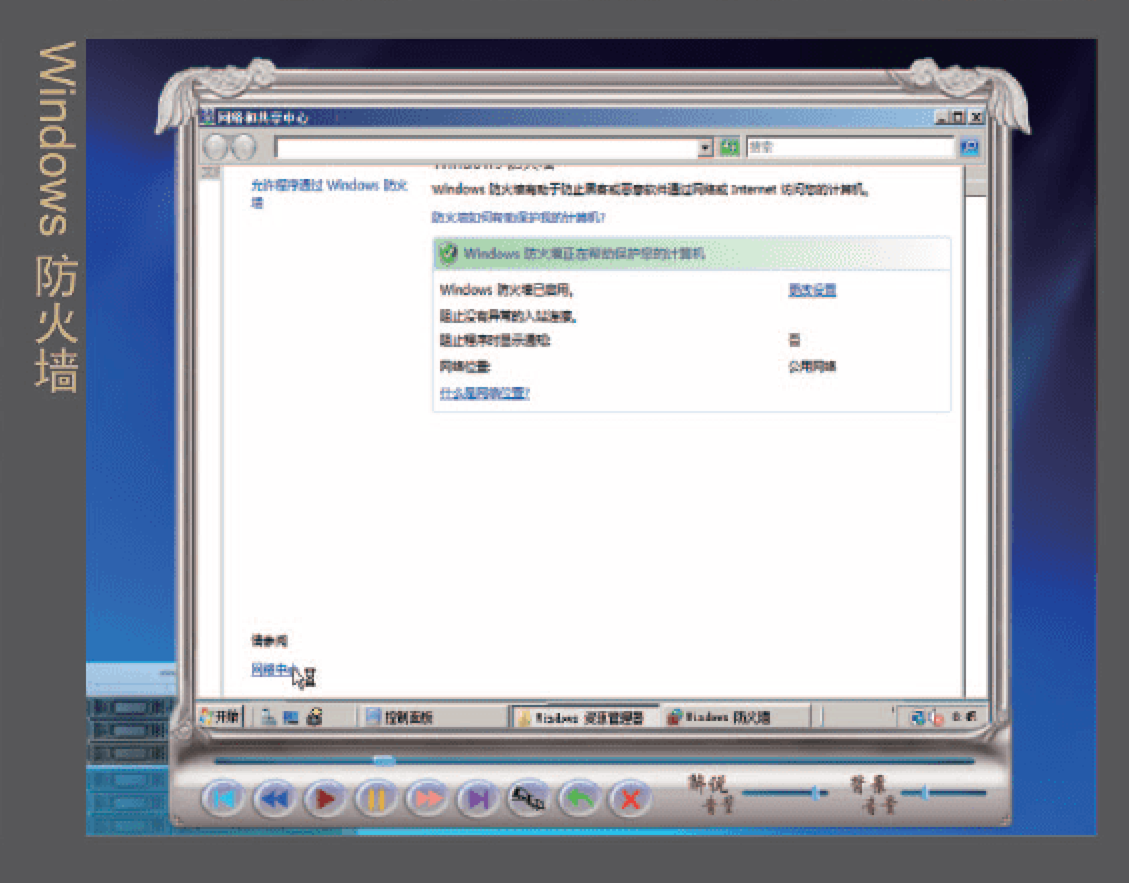
审核策略与事件日志



Internet信息服务安全



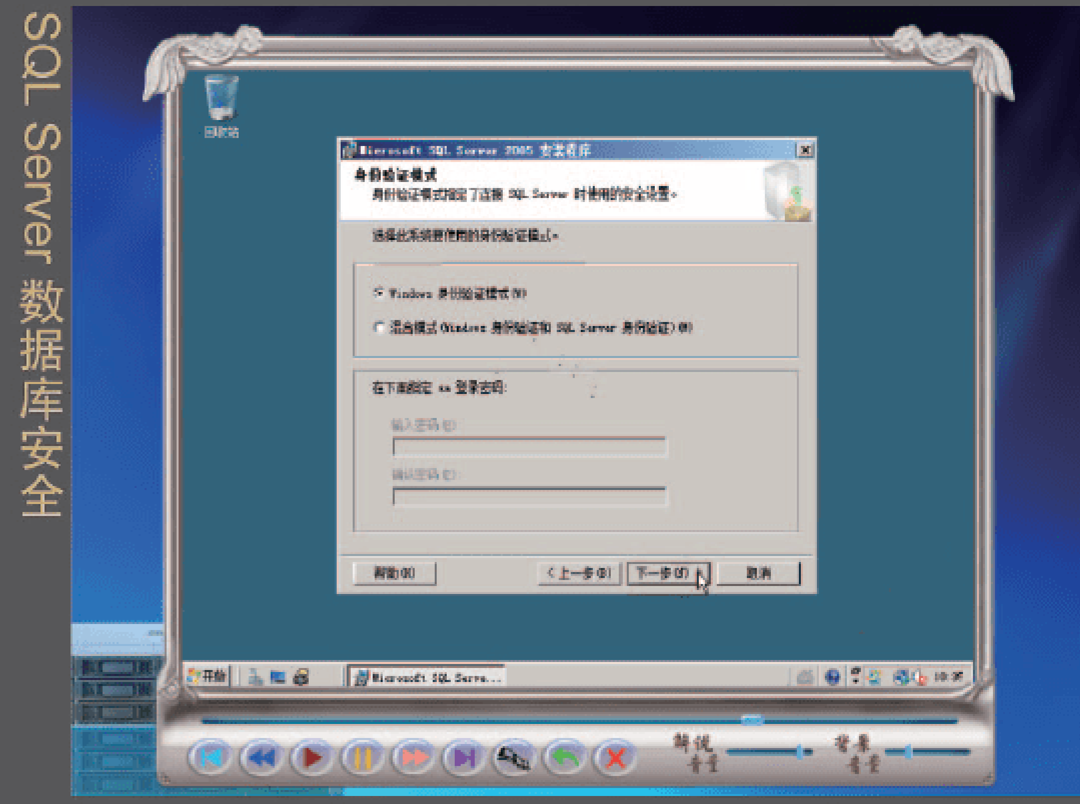
Windows 防火墙



Windows网络访问保护



SQL Server 数据库安全



360分钟

多媒体视频讲解

Windows Server 2008 系统安全管理实战指南

刘晓辉 李利军 编著

清华大学出版社

北　　京

内 容 简 介

本书系统全面地介绍了 Windows Server 2008 安全管理新特性，重点是在局域网络中的安全管理与设置技术。内容包括：Windows Server 2008 系统安全概述、Windows Server 2008 用户环境安全设置、修补系统漏洞、活动目录安全、用户帐户安全、组策略安全、数据存储安全、文件访问安全、服务器信息备份与还原、电子证书和认证服务、系统服务安全、端口安全、审核策略与事件日志、Internet 信息服务安全、Windows 防火墙、Windows 网络访问保护、SQL Server 数据库安全和 Windows Server 2008 系统安全新技术等。

本书完全站在实用的角度，突出实战技能的培养，并提供具有针对性的实验性课题和配套的多媒体教学光盘，适合具有一定网络知识水平的读者，及所有准备从事网络、系统管理，特别是网络安全管理的技术爱好者，同时，可作为企事业单位网络技术部门的参考用书，也可作为培训机构的教学用书。

图书在版编目（CIP）数据

Windows Server 2008 系统安全管理实战指南/刘晓辉，李利军编著.
—北京：清华大学出版社，2010.01

ISBN 978-7-302-21259-1

I. W… II. ①刘… ②李… III. 服务器－操作系统（软件），Windows Server 2008－安全技术 IV. TP316.86

中国版本图书馆 CIP 数据核字（2009）第 180417 号

责任编辑：夏非彼　廖闵闽
责任校对：宋英杰
责任印制：
出版发行：清华大学出版社　　**地　址：**北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　编：**100084
社 总 机：010-62770175　　**邮　购：**010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：
装 订 者：
经　销：全国新华书店
开　本：190×260　**印　张：**33.5　**插　页：**4　**字　数：**815 千字
附光盘 1 张
版　次：　**印　次：**
印　数：
定　价：

前　言

Windows Server 2008 操作系统最突出的改进就是安全性的提升。从理论角度对系统安全进行定义，Windows Server 2008 系统安全概述、Windows Server 2008 用户环境安全设置、修补系统漏洞、活动目录安全、用户帐户安全、组策略安全、数据存储安全、文件访问安全、服务器信息备份与还原、电子证书和认证服务、系统服务安全、端口安全、审核策略与事件日志、Internet 信息服务安全、Windows 防火墙、Windows 网络访问保护和 SQL Server 数据库安全，针对系统中涉及的安全问题，有目的和针对性地给出了相应的解决方案，最大限度地介绍了系统中所有有关安全的因素以及局域网的安全管理体系。

本书从 Windows Server 2008 提供的基础服务入手，完全以 Windows 操作系统安全的实际应用为基础，阐述了操作系统安全配置和管理在网络安全中起到的决定性作用，使读者能够全面提升网络的安全水平，迅速成长为合格的安全管理员。

本书共分 18 章，从 Windows Server 2008 安装到每种服务器的安装和配置，全面阐述了系统安全在实际应用中的部署方法。

第 1 章　Windows Server 2008 系统安全概述：介绍系统安全的定义以及系统可能遇到的威胁。

第 2 章　Windows Server 2008 用户环境安全设置：介绍如何安装并设置一个安全的操作系统。

第 3 章　修补系统漏洞：介绍漏洞的定义以及漏洞扫描、预警和修补等。

第 4 章　活动目录安全：介绍 Active Directory 相关安全措施。

第 5 章　用户帐户安全：介绍如何安全地设置帐户。

第 6 章　组策略安全：介绍使用组策略发布安全策略。

第 7 章　数据存储安全：讲解如何保护系统中磁盘的安全以及磁盘的备份和还原。

第 8 章　文件访问安全：讲解如何保护系统中的文件以及数据的安全共享设置。

第 9 章　服务器信息备份与还原：介绍服务器角色、注册表、网络配置和磁盘配额的备份与还原。

第 10 章　电子证书和认证服务：介绍电子证书和认证服务的基本知识，及其安装、备份和管理应用。

第 11 章　系统服务安全：介绍了合理配置系统服务，保持计算机的安全性。

第 12 章　端口安全：介绍了常用端口的安全配置，开启、禁用以及扫描等。

第 13 章　审核策略与事件日志：介绍审核、事件和日志概述，及相关的安全设置。

第 14 章　Internet 信息服务安全：介绍了基于 IIS 组件的 Web 服务器、FTP 服务器以及站点的安全配置。

第 15 章　Windows 防火墙：介绍了使用 Windows 防火墙保护系统安全的设置。

第 16 章　Windows 网络访问保护：介绍了服务器操作系统访问网络的安全设置。

第 17 章　SQL Server 数据库安全：介绍了数据库的安全设置以及数据库的备份与恢复。

第 18 章　Windows Server 2008 系统安全**新技术：**介绍系统新增安全功能、升级的安全特性以及应用服务器角色安全新特性。

本书由刘晓辉、李利军编著，李书满、吴琪菊、余素芬、吴海燕、赵敏捷、费一峰、毛向城、朱志明、朱春英、彭文芳、陈飞、傅维佳、张建、李海宁、陈志成、田俊乐、刘国增、王延杰、刘红等也参与了本书部分章节的编写工作。虽然作者在写作过程中已经高度注意到书中相关细节问题，但疏漏和不足之处恐难避免，敬请广大读者批评指正。

编　者

2010 年 01 月

目　录

第 1 章

Windows Server 2008 系统安全概述

Windows Server 2008 是微软公司鼎力推出的一个服务器操作系统，它代表了下一代 Windows Server。Windows Server 2008 在虚拟化工作负载、支持应用程序和保护网络方面向组织提供最高效的平台。从工作组到数据中心，从强大的网络功能到系统安全性，Windows Server 2008 都提供了令人兴奋且很有价值的新功能，对基本操作系统做出了重大的改进。该服务器系统安全工作涉及范围宽广，如系统内核安全、应用程序安全、用户帐户安全和端口安全等多个方面。根据服务器所处环境的不同，Windows Server 2008 系统支持管理员启用不同的安全防护策略。

本章导读

- Windows Server 2008 的版本及新特性
- Windows Server 2008 的硬件需求及安装方式
- Windows Server 2008 的初始配置
- Windows Server 2008 系统安全

Windows Server 2008

1.1 Windows Server 2008 概述

使用 Windows Server 2008，可使 IT 专业人员对其服务器和网络基础结构的控制能力更强，从而可重点关注关键业务需求。通过加快 IT 系统的部署与维护、使服务器和应用程序的合并与虚拟化更加简单，Windows Server 2008 为 IT 专业人员提供了更大的灵活性，而且其通过加强操作系统和保护网络环境提高了安全性。因此，Windows Server 2008 为任何组织的服务器和网络基础结构奠定了最好的基础。

1.1.1 Windows Server 2008 的版本

Microsoft 公司先后发布了多个版本的 Windows Server 2008，用于满足各种规模企业网络对服务器操作系统需求。其中，比较常用的版本有 6 个，另外还有 3 个不支持 Windows Server Hyper-V 技术的版本。

1. Windows Server 2008 Standard

Windows Server 2008 Standard 内置的强化 Web 和虚拟化功能，是专为增加服务器基础架构的可靠性和弹性而设计，亦可节省时间及降低成本。利用其强大的功能，让用户可以更好地控制服务器，同时大大简化了配置和管理任务；而先进的安全性和可靠性，可以强化操作系统，确保网络访问的安全。

2. Windows Server 2008 Enterprise

Windows Server 2008 Enterprise 可提供企业级的平台，部署企业关键应用。其所具备的群集和热添加（Hot-Add）处理器功能，可以增强可用性，而整合的身份管理功能，可以改善安全性，利用虚拟化授权权限整合应用程序，则可以减少基础架构的成本，因此 Windows Server 2008 Enterprise 可以为高度动态、可扩充的 IT 基础架构，提供良好的基础。

3. Windows Server 2008 Datacenter

Windows Server 2008 Datacenter 所提供的企业级平台，可在小型和大型服务器上部署具企业关键应用及大规模的虚拟化。其所具备的群集和动态硬件分割功能，可改善可用性，而通过无限制的虚拟化许可授权来巩固应用，可减少基础架构的成本。此外，此版本可以同时支持 x86 和 x64 的处理器，因此 Windows Server 2008 Datacenter 可以提供良好的基础，用于建立企业级虚拟化和扩充解决方案。

4. Windows Web Server 2008

Windows Web Server 2008 是特别为单一用途 Web 服务器而设计的系统，整合了重新设计架构的 IIS 7.0、ASP.NET 和 Microsoft .NET Framework，以便满足任何企业快速部署网页、网、



Web 应用程序和 Web 服务的需求。

5. Windows Server 2008 for Itanium-Based Systems

Windows Server 2008 for Itanium-Based Systems 已针对大型数据库、各种企业和自订应用程序进行优化，可提供高可用性和高可扩充性，能符合高要求且具关键性的解决方案的需求。

6. Windows HPC Server 2008

Windows HPC Server 2008 具备的高效能运算（HPC）特性，提供企业级的工具，建立高生产力的 HPC 环境。由于其建立于 Windows Server 2008 及 64 位技术上，因此，可有效地扩充至数以千计的处理核心，并可提供管理控制台，协助管理员主动监督和维护系统健康状况及稳定性。其所具备的工作排程之互操作性和弹性，可让 Windows 和 Linux 的 HPC 平台间进行整合，也可支持批次作业以及服务导向架构（SOA）工作负载，而增强的生产力、可扩充的效能以及使用容易等特色，可使 Windows HPC Server 2008 成为同级中最佳的 Windows 环境。

1.1.2　Windows Server 2008 的新特性

Windows Server 2008 相对于其他版本的 Windows 服务器系统，增加了许多新特性，对硬件支持能力更强，可以为用户提供更高的安全性和更加稳定的运行平台。Windows Server 2008 中的新特性，主要表现在以下几个方面：

1. IIS 7.0

Windows Server 2008 操作系统绑定了 IIS 7.0，这也是 Windows Server 2008 中的大规模改进之一，相对于 IIS 6.0 而言，是最具飞跃性的升级产品，通过委派管理、增强的安全性和缩小的攻击面、Web 服务的集成应用程序以及改进的管理工具等关键功能，提高了安全性和管理性。例如，Web 站点的管理权限更加细化，可以将各种操作权限委派给指定管理员，极大的优化了网络管理，大大节省了管理员的时间。

2. 核心服务器

Windows Server 2008 提供了 Server Core 功能，和 Linux 操作系统一样，只提供基本的服务器功能。

Server Core 是 Server 2008 的最小版本，这是一个不包含服务器图形用户界面的操作系统，提高了稳定性，只安装必要的服务和应用程序，提供 DHCP、DNS 等基础网络服务。与完整版本的系统相比，由于服务器上安装和运行的程序和组件较少，暴露在网络上的攻击面也较少，因此更安全，也可减少维护和管理的时间。

3. 网络访问保护（NAP）

网络访问保护（NAP）可允许网络管理员自定义网络要求，并限制不符合这些要求的计算机访问网络。NAP 强制执行管理员定义的正常运行策略，这些策略包括连接网络的计算机的软件要求、安全更新要求和所需的配置设置等内容。Windows Vista SP1，Windows XP SP3

都包含来自 Server 2008 的 NAP，由此可见它的重要性。

NAP 强制实现方法支持四种网络访问技术，与 NAP 结合使用来强制实现正常运行策略，包括：Internet 协议安全（IPsec）强制、802.1X 强制、用于路由和远程访问的虚拟专用网络（VPN）强制以及动态主机配置协议（DHCP）强制。

4. 只读域控制器（RODC）

这是 Windows Server 2008 操作系统提供的一种新类型的域控制器，可以在域控制器安全性无法保证的位置轻松部署域控制器，降低了在无法保证物理安全的远程位置（如分支机构）中部署域控制器的风险。RODC 维护 Active Directory 目录服务数据库的只读副本，通过将该数据库副本放置在更接近分支机构的地方，使用户可以更快地登录，即使处于没有足够物理安全性来部署传统域控制器的环境，也能更有效地访问网络上的身份验证资源，在提高了可靠性和安全性的同时还减少了流量消耗。

5. 虚拟服务器

通常情况下，多数服务器 85%的 CPU 机时都是处于闲置状态的，为了尽量减少资源浪费，充分发挥服务器性能，Windows Server 2008 系统中引进了虚拟化技术。通过 Windows Server 2008 内置的服务器虚拟技术，可以在单个服务器上虚拟 Windows、Linux 等多个操作系统，并与现有环境互操作。利用更加简单、灵活的授权策略，可以更容易地利用虚拟化的各种优势。用户利用虚拟化技术就像所有应用程序都运行在自己电脑上一样，可以明显节省成本和提高硬件使用率，同时可以优化基础结构并提高服务器可用性。

6. 全新的命令行工具

PowerShell 原计划作为 Windows Vista 的一部分，但只是免费下载的增强附件，随后又成了 Exchange Server 2007 的关键组件，接下来又是 Windows Server 2008 不可或缺的一个成员。这个新的命令行工具可以作为图形界面管理的补充，也可以彻底取代它。

7. BitLocker 驱动器加密

BitLocker 驱动器加密是 Windows Server 2008 中一个重要的新功能，可保护服务器、工作站和移动计算机。BitLocker 可对磁盘驱动器的内容加密，防止未经授权的使用者绕过文件和系统保护，或者对存储在受保护驱动器上的文件进行脱机查看。

8. 自修复 NTFS 文件系统

在 Windows Server 2008 中，将有一个新增的系统服务在后台检测文件系统的错误，并且在服务器运行状态下进行直接修复。如果检测服务正在修复损坏的磁盘结构，服务器只会暂时无法访问部分数据，在修复结束后即可重新访问。系统是永远不会关闭的，通常无需使用 CHKDSK（全称 check disk，即磁盘检查）检测磁盘。

9. 并行会话的创建

在 Windows Server 2008 之前的操作系统中，默认是以串行方式创建会话的。也就是说，当多个用户同时登录终端系统时会造成系统的瓶颈，造成用户排队等待会话的初始化。在



Windows Vista 及 Windows Server 2008 中的新会话模块，至少可以同时初始化 4 个会话，如果有 4 块以上的会话模块，还可以增加更多。Windows Vista 下的 Media Center 就是一个很好的例子，如果在多个不同的房间同时启动 Media Center 就会发现，速度要比 Windows XP 下的 Media Center 更流畅。

10. 快速关机服务

在其他版本的 Windows 系统中，关机速度都比较缓慢。在 Windows XP 中，一旦关机开始后系统就会启动一个 20 秒的计数器，超时后会询问用户是否结束应用程序。在服务器系统中，该计数器是应用程序的生命之钟。而在 Windows Server 2008 下，这 20 秒的倒计时被一个专门的服务取代了，该服务会向需要关闭的程序不间断的送达关机信号，直至程序回应自己确实已退出为止。

11. 内核事务管理器

这对开发人员们而言尤为重要，即使无法完全排出，也能在最大程度上减少多个线程访问同一系统资源（注册表、文件系统等）时的死锁问题。以数据库系统为例，交互指令都会按次序插入内存队列，并最终一次性执行。内核事务管理器的目的是方便进行大量的错误恢复工作，它允许事务客户端的插入（plug into），事务客户端通过这样的方式来使用内核事务管理器所管理的资源。

12. SMB2 网络文件系统

SMB（Server Message Block，服务器信息模块）在很早以前就成为了 Windows 自带的网络文件系统。随着多媒体文件体积的日渐巨增，对服务器的要求也相应的增加了。在微软的内部测试中 SMB2 的速度比 Windows Server 2003 中的网络文件系统要快 4~5 倍，相当于 400%的效率提升。

13. 地址空间的随机加载

ASLR（Address Space Layout Randomization，地址空间配置随机化）或许是 Windows Vista 中最具争议的一项功能，它直接导致了操作系统的任何两个并发实例每次都会载入到不同的内存地址上。微软表示，这项功能不会影响普通的系统服务，所以不必担心应用程序无法链接到需要使用的服务。恶意软件其实就是一堆不守规矩的代码，不会按照操作系统要求的正常程序执行，经常利用早期 Windows 版本在固定内存地址加载文件上的缺陷，能够找到在 32 位的 Windows XP SP2 下哪里装载着 KERNEL32.DLL，并随意的进行访问。因为不管任何机器在任何时候启动，这个 DLL 每次都会被载入同一个内存空间地址，所以非常容易恶意利用。而现在有了 ASLR，系统会在启动时从 256 个随机位置中选取一个，并附加 16M 空间的（正或负）偏移，恶意软件能找到这些位置的机会可以说是相当的渺茫。

14. Windows 硬件错误体系

微软的确开始将 Windows 错误进行标准化，确切地说是应用程序向系统报告错误的一种协议。在过去，设备报告其错误的方式多种多样，各种硬件系统之间没有既定的标准。直至今日，要编写一个按照统一模式来整理和显示各种错误的程序也是极其困难的，因为不同的错误源有不同的错误代码。而在 Windows Server 2008 里，所有的硬件相关错误都使用同样的界面

汇报给系统，第三方软件就能轻松管理、消除错误，管理工具的发展也会更轻松。

15. 下一代加密技术（CNG）

CNG（Cryptography Next Generation）加密技术提供了灵活的加密开发平台，允许 IT 专业人员在与加密相关的应用程序（如 Active Directory 证书服务、安全套接字层（SSL）和 Internet 协议安全（IPSec））中创建、更新和使用自定义加密算法。

1.1.3 Windows Server 2008 的硬件需求

虽然 Windows Server 2008 在搭建环境和其他特征上与 Window Server 2003 很相似，但还是有些地方需要特别注意，尤其是对于硬件配置的要求方面，如显示设备、网络适配器、光驱软驱、键盘鼠标等，均要保证与 Windows Server 2008 系统相兼容。如表 1.1 中列出的一些最开始安装时的配置建议。

表 1.1 Windows Server 2008 系统的硬件需求

相关信息	具体说明
处理器	最低 1.0GHz x86 或 1.4GHz x64 推荐 2.0GHz 或更高；安腾版则需要 Itanium 2
内存	最低 512MB 推荐 2GB 或更多
内存最大支持	32 位标准版 4GB、企业版和数据中心版 64GB 64 位标准版 32GB，其他版本 2TB
硬盘	最少 10GB，推荐 40GB 或更多 内存大于 16GB 的系统需要更多空间用于页面、休眠和转存储文件
备注	光驱要求 DVD-ROM； 显示器要求至少 SVGA 800×600 分辨率，或更高。

1.1.4 Windows Server 2008 安装前的准备

为了保证 Windows Server 2008 能够顺利安装，在开始安装前必须做好准备工作，包括检查日志错误、备份文件、断开网络以及断开非必要的硬件连接等。另外，Windows Server 2008 对硬盘空间要求比较大，系统分区至少为 10GB，不过，为了保证系统更好的运行、安装更新或其他软件做准备，建议设置为 40GB 或更大。

1. 切断与硬件设备的连接

如果计算机正与打印机、扫描仪或者不间断电源（UPS）等非必要的外设连接，则应在运行安装程序之前将其断开，避免安装程序在自动检测这类设备时出现问题。



2. 断开网络连接

网络中可能会有病毒在传播，如果不是通过网络安装操作系统，在安装之前就应断开网络连或直接拔下网线，以免新安装的系统又被感染上病毒。

3. 检查系统日志，寻找错误

如果在计算机中已经安装了其他操作系统，建议使用“事件查看器”查看系统日志，找出可能在升级期间引发问题的最新错误或重复发生的错误。

4. 备份数据

如果服务器中已安装有其他系统，为了避免丢失重要数据，建议在升级前备份有用的数据，包括计算机运行所需的全部数据和配置信息，以及所有的用户和相关数据，尤其是一些提供网络服务数据（例如 DHCP 数据等）。建议将文件备份到各种不同的媒体，例如，磁带驱动器或网络上其他计算机的硬盘，而尽量不要保存在本地计算机的磁盘中。

5. 检查硬件和软件兼容性

如果要将 Windows 2000 Server 或 Windows Server 2003 升级到 Windows Server 2008，为了保证应用程序的兼容性，可以使用“Microsoft 应用程序兼容性工具包”进行检测，并可用来准备安装 Windows Server 2008。

6. 加载驱动程序

由于服务器中往往安装有 RAID 卡等设备，而这些设备可能无法被 Windows 系统所识别，因此，必须在安装之前就加载相应的驱动程序。大多数品牌服务器出厂时就已经配备了引导光盘，用来加载各种驱动程序并引导安装 Windows Server 2003。因此，建议使用引导光盘安装。如果没有引导光盘，那么，安装操作系统之前可以只加载 RAID 控制器的驱动程序，否则，无法安装操作系统。至于其他设备的驱动程序，可以在系统安装完成后再安装。

7. 使用 DVD 光驱

由于 Windows Server 2008 安装程序比较大，安装光盘采用的是 DVD 格式，因此，服务器必须配备 DVD 光驱，VCD 无法读取。

1.1.5　Windows Server 2008 的安装方式

Windows Server 2008 可以采用多种方式安装，不同的安装方式分别适用于不同的环境，选择合适的安装方式，可以更加顺利地安装好系统。一般情况下，可以通过如下几种方法安装 Windows Server 2008 操作系统：

1. 全新安装

使用 CD 启动计算机并进行安装，这是最基本的方法，也为绝大部分计算机所支持。全新

安装或者重新安装服务器时，往往会用到服务器厂商提供的引导光盘或工具盘，然后根据提示信息适时插入 Windows Server 2008 安装光盘即可。

2. 升级安装

如果计算机中原来安装的是 Windows 2000 Server 或 Windows Server 2003 等操作系统，可以直接升级成 Windows Server 2008，此时不需要卸载原来的 Windows 系统，只要在原来的系统基础上进行升级安装即可，而且升级后还可保留原来的配置。

从不同版本的 Windows Server 2003 可以升级到相应版本的 Windows Server 2008。如表 1.2 列出了不同版本操作系统的升级原则。

表 1.2 Windows Server 2003 升级原则

当前系统版本	可以升级到的 2008 版本
Windows Server 2003 R2 标准版 Windows Server 2003 标准版（SP1） Windows Server 2003 标准版（SP2）	Windows Server 2008 标准版 Windows Server 2008 企业版
Windows Server 2003 R2 企业版 Windows Server 2003 企业版（SP1） Windows Server 2003 企业版（SP2）	Windows Server 2008 企业版

3. 通过 Windows 部署服务远程安装

与 Windows 2000/2003 一样，Windows Server 2008 也支持通过网络从 Windows 部署服务器远程安装，并且可以通过应答文件实现自动安装。当然，服务器网卡必须具有 PXE（预引导执行环境）功能，可以从远程引导。

1.2 Windows Server 2008 的初始配置

安装 Windows Server 2008 与 Windows Server 2003 最大的区别就是，在安装过程中无需设置计算机名、网络连接等信息，所需时间也大大减少。不过，在安装完成后，就应该设置计算机名和 IP 地址、配置 Windows 防火墙和自动更新等，这些均可在“初始配置任务”或“服务器管理器”中完成。

1.2.1 启用 Windows 防火墙

Windows Server 2008 自带了 Windows 防火墙功能，可以有效地防止服务器上未经允许的程序与网络进行通信，从而在一定程度上保护了服务器与网络的安全。如果要允许某个程序与网络通信，可以将其添加到 Windows 防火墙的“例外”中。默认状态下，安装完 Windows Server 2008 系统以后，Windows 防火墙为开启状态。



01 依次打开“开始”→“控制面板”→“Windows 防火墙”，显示如图 1.1 所示“Windows 防火墙”窗口。

02 单击“更改设置”链接，或者单击“启用或关闭 Windows 防火墙”链接，显示如图 1.2 所示“Windows 防火墙设置”对话框，默认选择“启用”单选按钮，启用防火墙。如果连接到不太安全的网络，为了保护服务器的安全，可选中“阻止所有传入连接”复选框，可以阻止所有的程序与网络通信。选择“关闭”单选按钮则禁用防火墙。



图 1.1　“Windows 防火墙”窗口

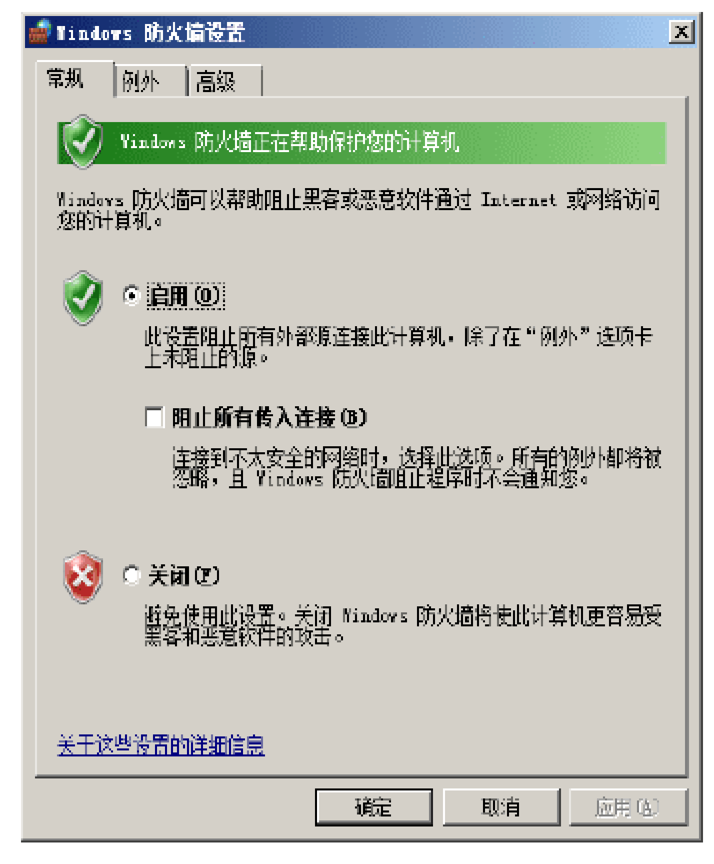


图 1.2　“Windows 防火墙设置”对话框

03 设置完成后，单击“确定”按钮保存即可。

1.2.2　配置自动更新

为了保护 Windows 系统的安全，微软公司会不定期发布各种更新程序，以修补系统漏洞，提高系统性能。因此，系统更新是 Windows 系统必不可少的功能。在 Windows Server 2008 服务器中，为了避免因漏洞而造成故障，必须启用自动更新功能，并配置系统定时或自动下载安装更新程序。

01 依次打开“开始”→“控制面板”→“Windows Update”，或者在“服务器管理器”窗口的“安全信息”区域中单击“配置更新”超链接，显示如图 1.3 所示“Windows Update”窗口。Windows Server 2008 安装完成后，默认没有配置自动更新。

02 单击“更改设置”链接，显示如图 1.4 所示“更改设置”窗口。在这里可以选择 Windows 安装更新的方法。如果选择“从不检查更新”单选按钮，则禁用自动更新功能。

03 单击“确定”按钮保存设置。Windows Server 2008 就会根据所做配置自动从 Windows Update 网站检测并下载更新。

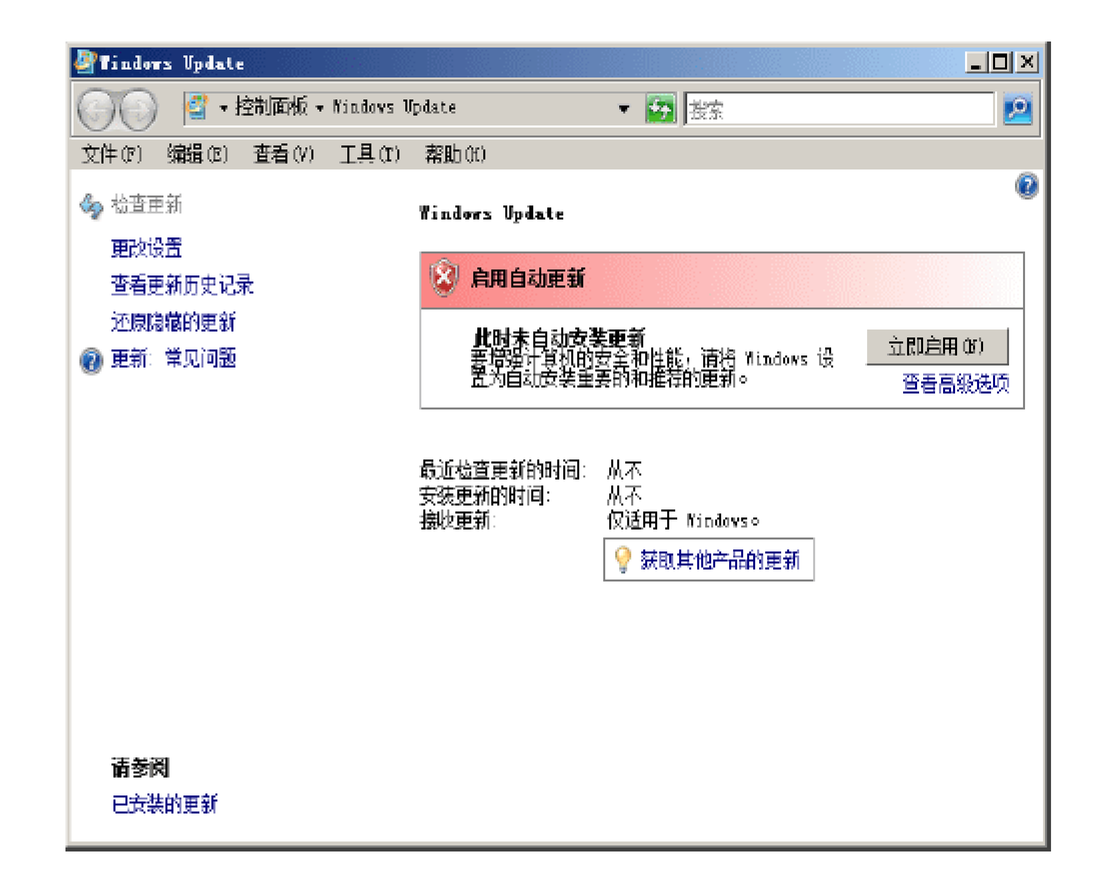


图 1.3 “Windows Update”窗口



图 1.4 “更改设置”窗口

1.3 Windows Server 2008 系统安全

启用 Windows 防火墙、配置 Windows Update 可以从一定程度上确保服务器系统的安全，但是对服务器上安装的应用程序、服务器角色起不到任何保护作用。为此，完成相应网络服务的部署之后，管理员应借助 Windows Server 2008 提供的安全配置向导，为指定服务或网络应用定制安全配置策略。

1.3.1 安全配置向导

安全配置向导（Security Configuration Wizard ，SCW）可以帮助管理员快速完成创建、编辑、应用和回滚安全策略操作。在 Windows Server 2008 系统中，已经默认集成安全配置向导，用户无需安装即可直接应用。

1. 注意事项

SCW 是一个完全基于服务角色的工具，用户可以根据需要创建针对某个服务器角色的安全策略，并且可以将其应用到其他相应类型的服务器上。配置和应用 SCW 时应注意以下几点：

- SCW 禁用不需要的服务并提供对具有高级安全性的 Windows 防火墙的支持；
- 使用 SCW 创建的安全策略与安全模板不同，其中前者扩展名为.xml，而后者扩展名为.inf。用户创建的安全策略源于安全模板，安全模板包含的安全设置可以应用于所有的服务器角色；
- 部署 SCW 安全策略后并不会影响服务器提供服务时所需的组件，并且应用之后，管理员仍可以通过服务器管理器安装所需的组件；
- 应用 SCW 安全策略之后，SCW 将自动选择所有从属角色；
- 创建和应用 SCW 安全策略时，应确保服务器的 IP 协议及端口配置完全正确。



2. 配置安全策略

01 依次选择“开始”→“管理工具”→“安全配置向导”命令，启动“欢迎使用安全配置向导”对话框。也可以在“开始”菜单的“开始搜索”文本框中输入 scw.exe 命令，来启动安全配置向导。

02 单击“下一步”按钮，显示“配置操作”对话框，选中“新建安全策略”单选按钮。单击“下一步”按钮，显示如图 1.5 所示“选择服务器”对话框。在“服务器”文本框中，输入需要进行安全配置的 Windows Server 2008 服务器的主机名或 IP 地址。也可以单击“浏览”按钮，选择需要进行安全配置的目标计算机。

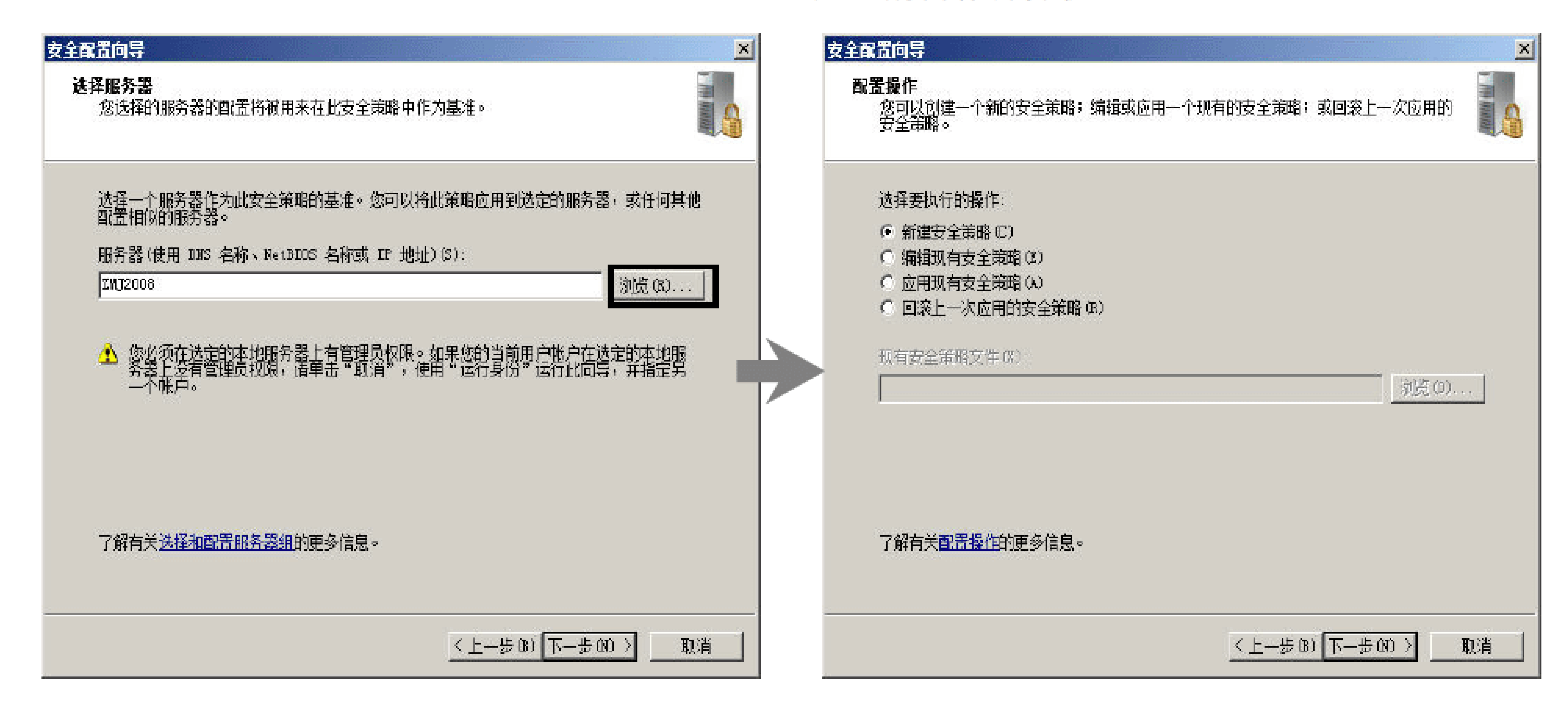


图 1.5　选择服务器

安全配置向导提供了 4 种配置操作：

- 创建新的安全策略。可以创建用于配置服务、Windows 防火墙、Internet 协议安全（IPsec）设置、审核策略和特定注册表设置的安全策略。安全策略文件是 XML 格式文件，默认保存路径为%systemroot%\security\msscw\Policies；
- 编辑现有安全策略。可以编辑已使用 SCW 创建的安全策略。必须先选择“编辑现有安全策略”，才能浏览到要编辑的安全策略文件所在的文件夹。编辑的策略可存储在本地上或网络共享文件夹中；
- 应用现有安全策略。使用 SCW 创建安全策略后，可将其应用到测试服务器，或者应用到生产环境；

提示



在将新创建或新修改的安全策略应用到生产环境之前，首先进行测试，然后将安全策略部署到业务系统中，测试可使新策略在生产环境中导致意外结果的可能性降至最低。

- 回滚上一次应用的安全策略。如果使用 SCW 应用的安全策略使服务器功能达不到预期的效果，或者导致其他非预期结果，则可以回滚该安全策略，将自动从该服务器删除对应的安全策略。



注意　如果策略是在“本地安全策略”中编辑的，在应用策略后，这些更改就不能回滚到应用前的状态。对于服务和注册表值，回滚过程还原了在配置过程中更改的设置。对于 Windows 防火墙和 IPSec，回滚过程取消当前使用的任何 SCW 策略的分配，并重新分配在配置时使用的前策略。

03 单击“下一步”按钮，开始扫描配置数据库，主要包括已安装或运行的网络服务、IP 地址及子网信息等。扫描完成显示如图 1.6 所示“正在处理安全配置数据库”对话框。单击“查看配置数据库”按钮，打开“SCW 查看器”对话框，在这里可以查看详细扫描结果。

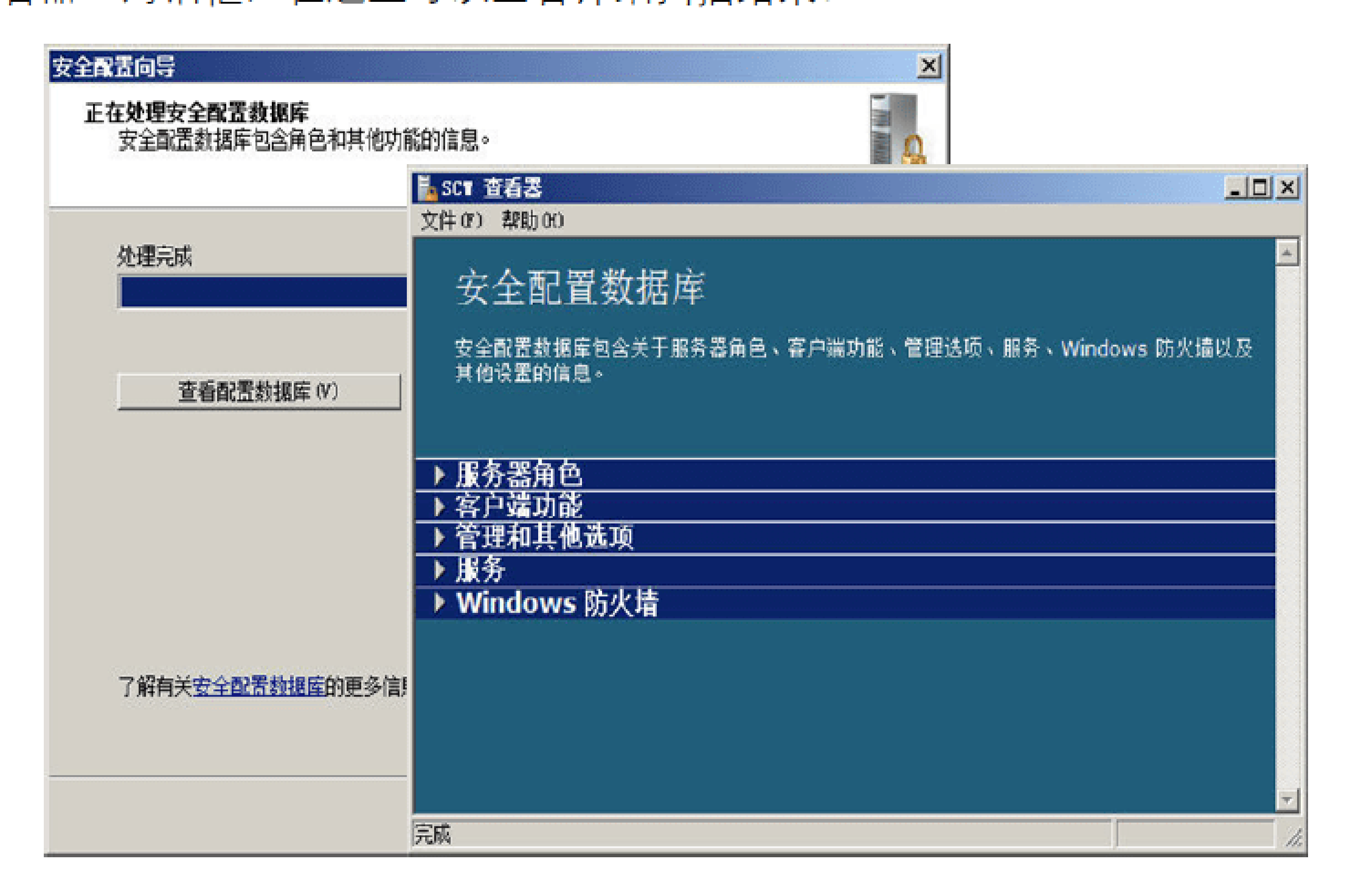


图 1.6　“正在处理安全配置数据库”对话框及数据库配置信息



提示　需要注意的是，在此过程中由于 Internet Explorer 7.0 的安全设置，可能会出现安全提示信息，单击“是”按钮跳过即可。

04 单击“下一步”按钮，显示“基于角色的服务配置”对话框。安全配置向导可以根据当前服务器提供网络服务的不同，配置相应的安全策略。依次单击“下一步”按钮，选择服务器角色、客户端功能和管理选项，如图 1.7 所示。



图 1.7　选择服务器角色、客户端功能和管理选项

在“选择服务器角色”对话框的“查看”下拉列表框中，提供了 4 种可供选择的抉择模式。



- 所有角色：列表框出所有的 Windows Server 2008 可以使用的角色列表框；
- 安装的角色：列出当前服务器中已经安装的角色，包括没有设置的角色；
- 未安装的角色：列出当前服务器中没有安装的角色，不包括没有设置的角色；
- 选定的角色：列出当前服务器中已经选定的角色。

注意　为了保证服务器的安全，仅选择所需要的服务器角色即可，如本例中只选择“Web 服务器”。选择多余的服务器角色，会增加 Windows Server 2008 系统的安全隐患。

05 依次单击“下一步”按钮，配置其他服务、未指定的服务、确认对服务的更改，从而完成对指定服务器角色的安全策略配置，如图 1.8 所示。其中在“处理未指定的服务”对话框中，提供了两种处理方式，其区别如下：

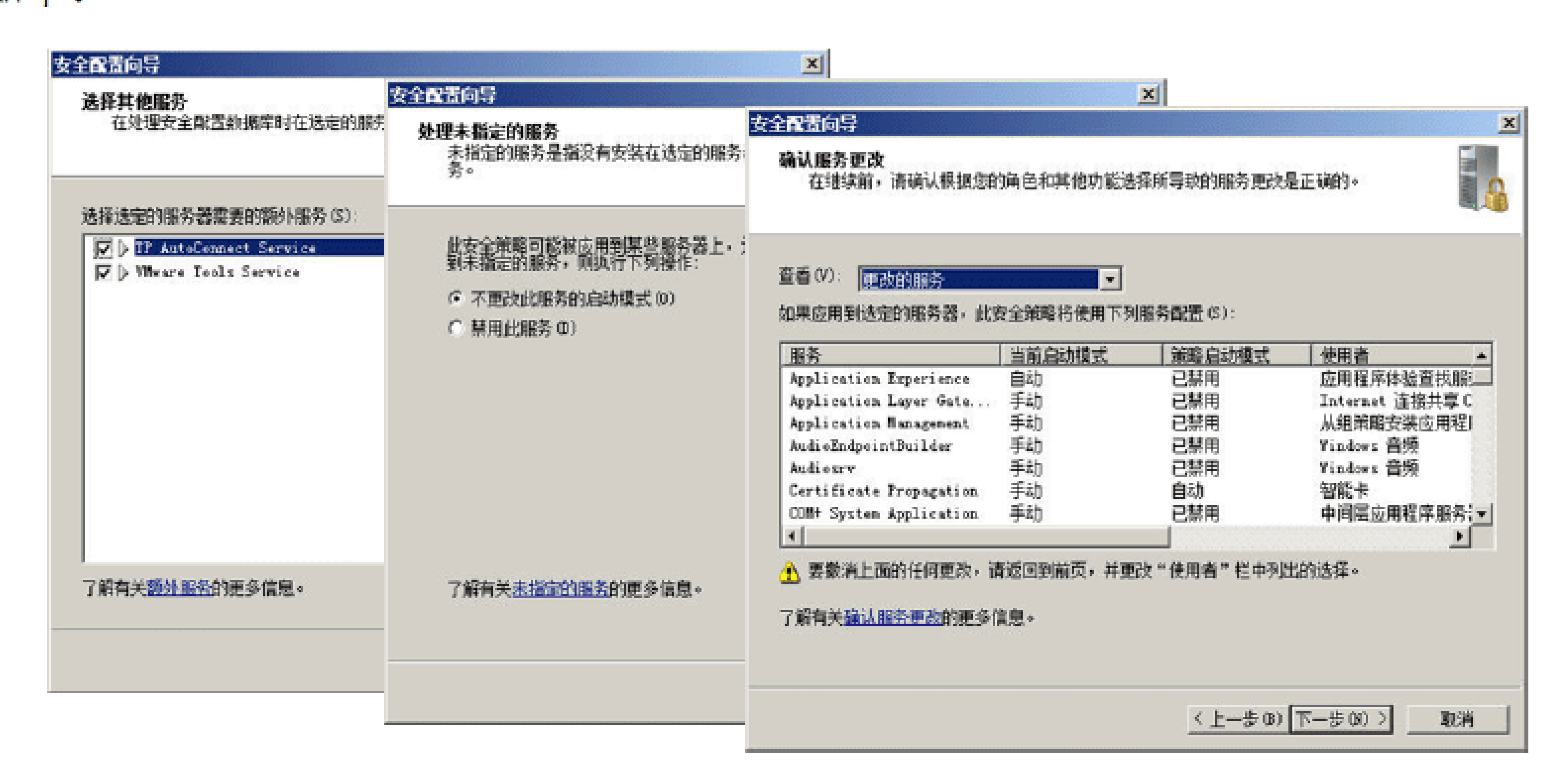


图 1.8　选择其他服务和未指定的服务

- 保持服务的当前启动模式。如果选择此选项，则在应用此安全策略的服务器上启用的未指定服务将保持启用状态，而禁用的那些服务将保持禁用状态；
- 禁用服务。如果选择此选项，则不在安全配置数据库中的或未安装在选定服务器上的所有服务都将被禁用。

06 单击“下一步”按钮，显示“网络安全”对话框，开始配置与服务器角色相关的 Windows 防火墙规则，建议不要跳过此步骤。依次单击“下一步”按钮，设置网络安全规则，如图 1.9 所示。



图 1.9　配置网络安全选项

如果“网络安全规则”列表中没有列出需要使用的 Windows 防火墙规则，可以单击“添加”按钮，打开如图 1.9 所示“添加规则”对话框，将其添加到列表中。在“名称”文本框中，输入防火墙规则的名称，如 www，为了便于区分还可以输入相关的描述信息；在“方向”选项框中，选择“入站”单选按钮；另外，还可以根据需要在“操作”选项框中选择相应限制连接方式。

07 单击“下一步”按钮，显示“注册表设置”对话框。通过该设置可以修改 Windows Server 2008 服务器注册表中一些特殊键值，从而严格限制用户的访问权限。建议用户不要跳过此步骤。单击“下一步”按钮，配置 SMB 安全签名选项，如图 1.10 所示。



图 1.10　设置注册表和 SMB 安全签名选项

08 依次单击“下一步”按钮，设置出站身份验证方法、使用的用户帐户类型和确认注册表设置摘要，如图 1.11 所示。如果是在域网络中进行远程登录，在“出站身份验证方法”对话框中，选中“域帐户”复选框即可；如果是工作组环境，建议选中“远程计算机上的本地帐户”复选框。

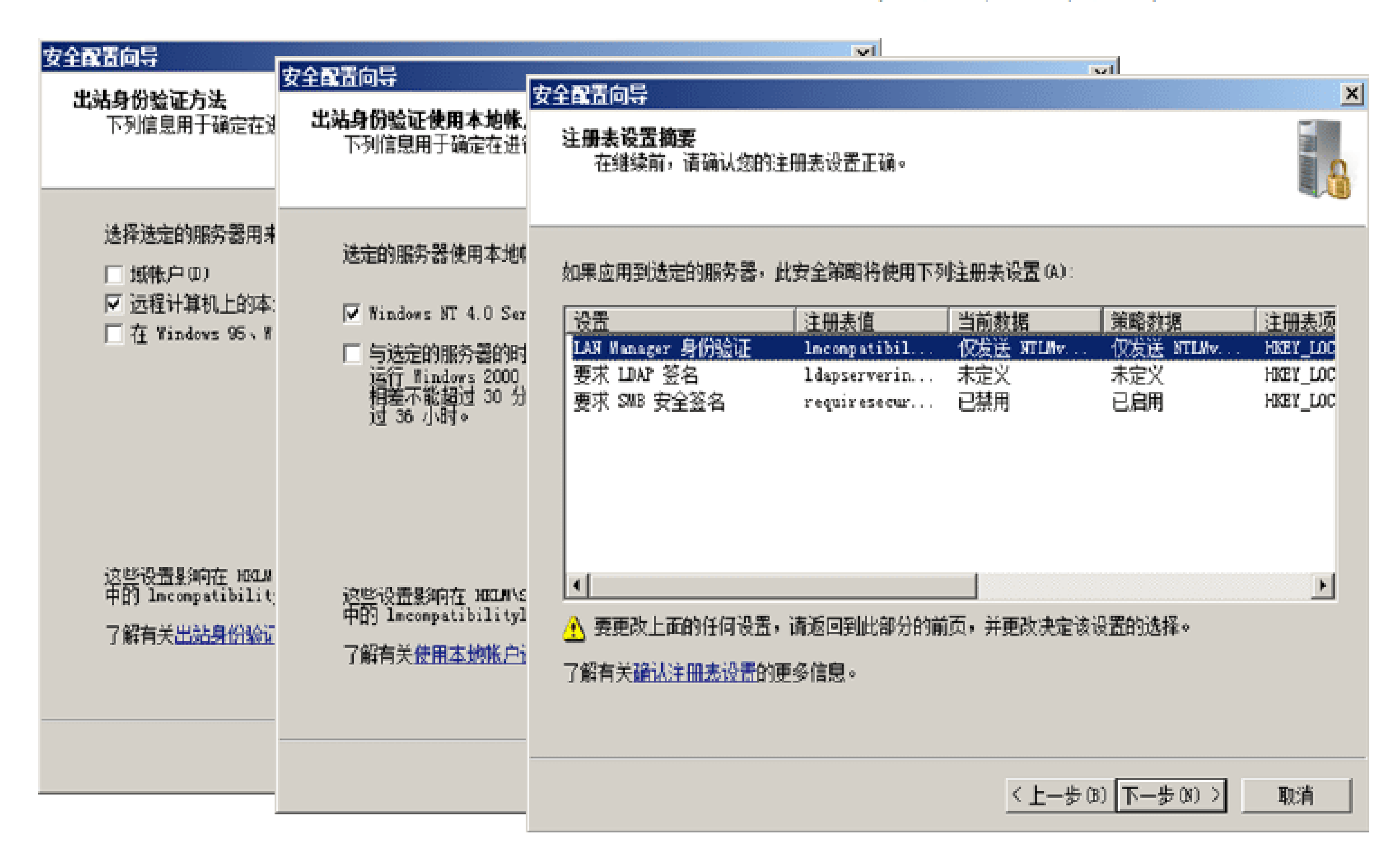


图 1.11　出站身份验证方法和用户帐户类型

09 单击“下一步”按钮，显示“审核策略”对话框。Windows 审核策略主要用于审核日志记录中的相关内容，并确定受影响的系统对象。安全策略回滚功能是无法回滚安全向导中的审核策略设置的。依次单击



“下一步”按钮，设置系统审核策略和确认审核策略摘要即可，如图 1.12 所示。

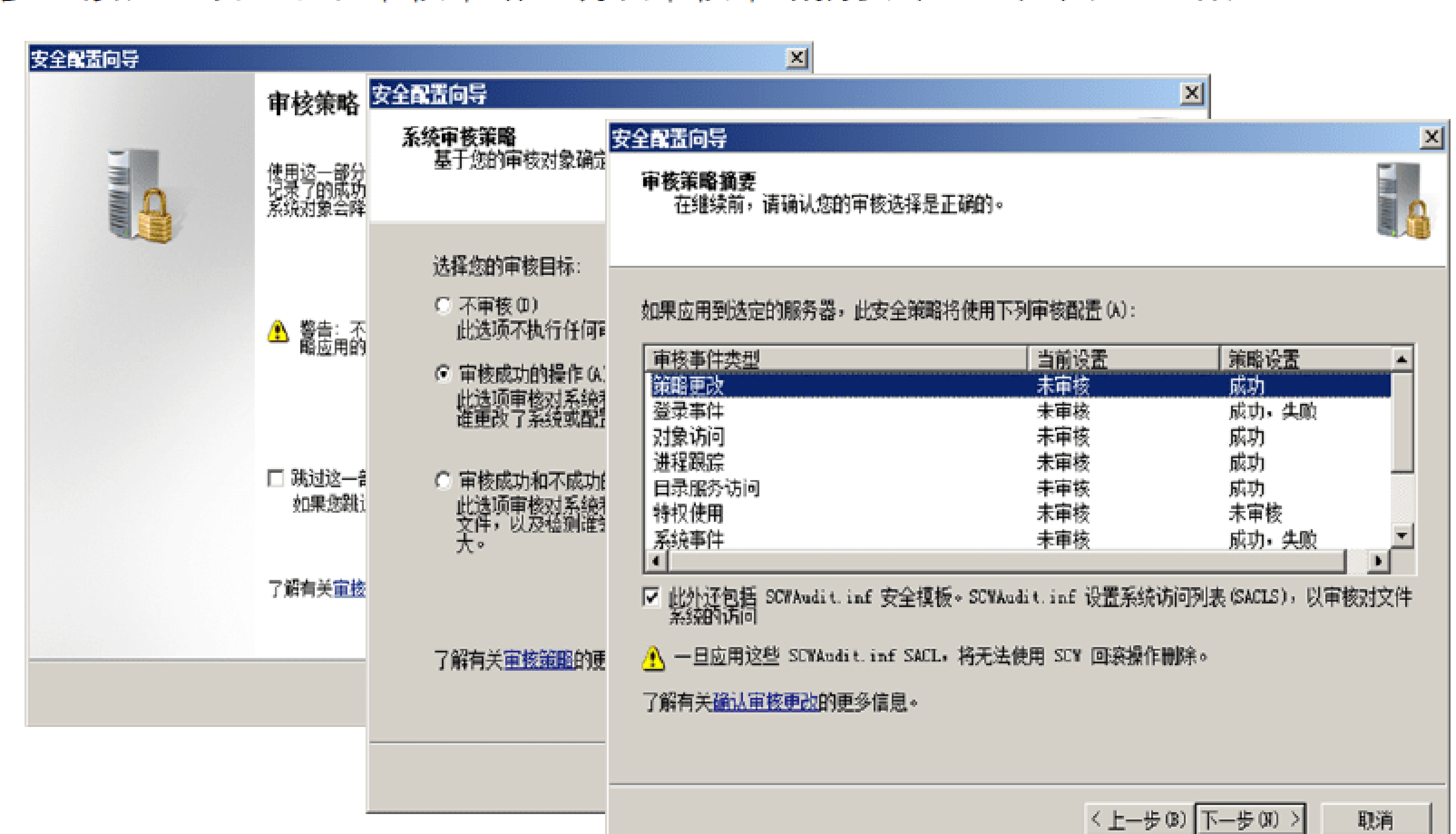


图 1.12　设置审核策略

10 单击“下一步”按钮，显示“保存安全策略”对话框。保存之后，即可将该安全策略应用到当前或其他服务器上。单击“下一步”按钮，设置安全策略文件名及保存路径，如图 1.13 所示。

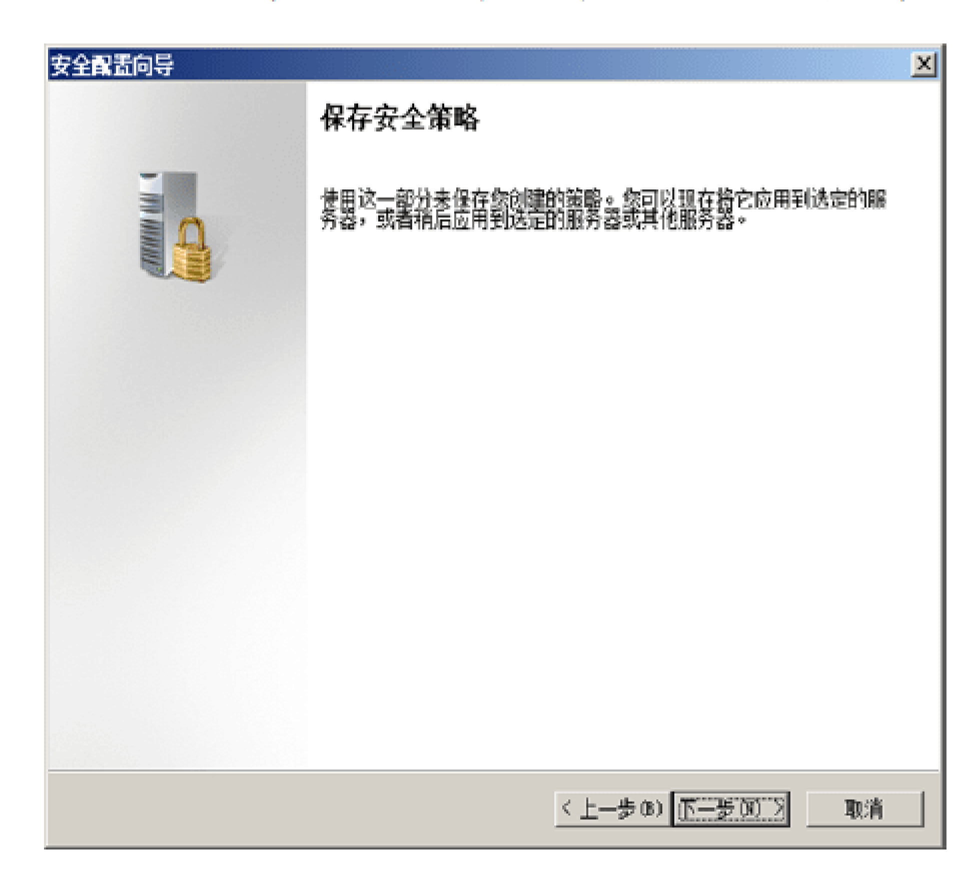




图 1.13　保存安全策略



提示　单击“包括安全模板”按钮，还可以向当前安全策略中添加其他安全模板中的安全规则，这些规则将拥有较高的优先级。SCW 回滚功能将无法回滚已经应用的策略模板中的规则设置。

11 单击“下一步”按钮，显示如图 1.14 所示“应用安全策略”对话框。如果选中“现在应用”单选按钮，可以将安全策略立即应用到当前服务器；建议选择“稍后应用”单选按钮，测试之后再应用到服务器。

12 单击“下一步”按钮，显示如图 1.15 所示“正在完成安全配置向导”对话框。单击“完成”按钮，完成安全策略的设置。



图 1.14 “应用安全策略”对话框

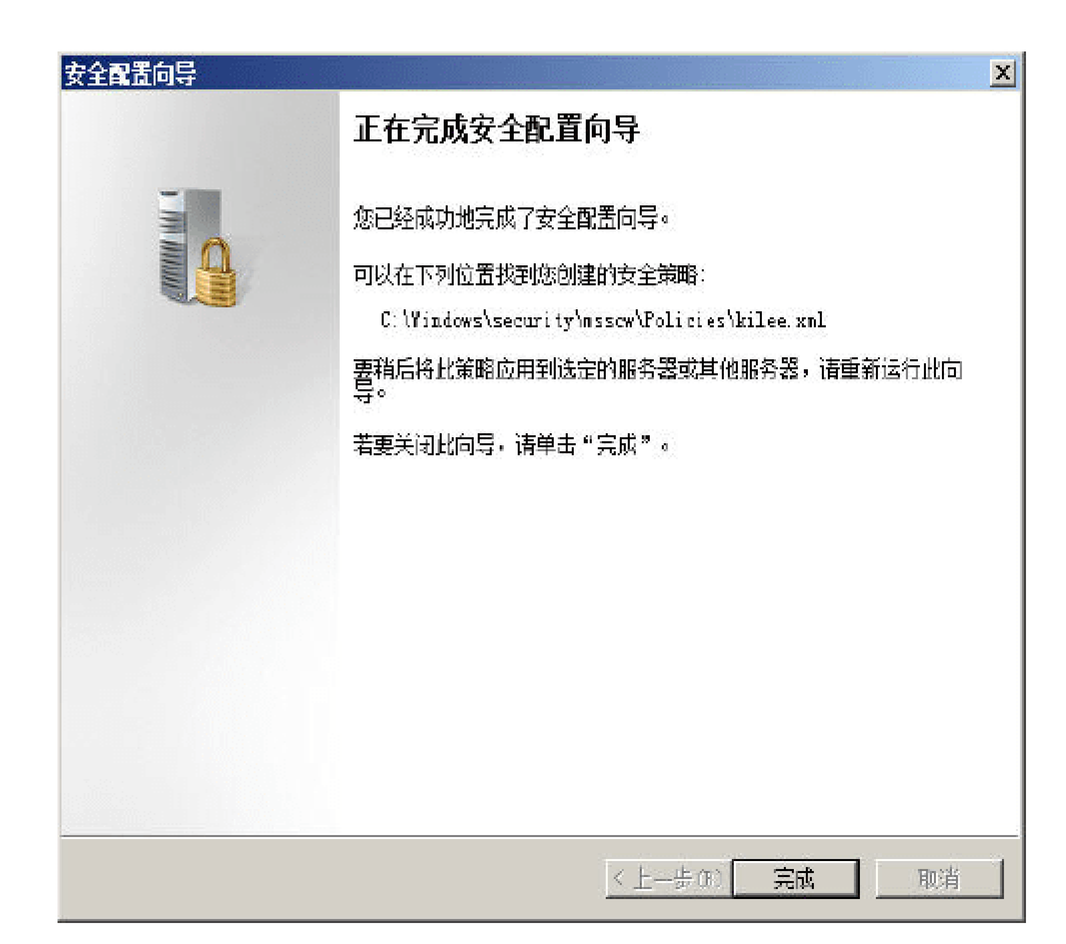


图 1.15 “正在完成安全配置向导”对话框

3. 应用安全配置策略

使用安全配置向导创建的安全策略，可直接应用于所有运行 Windows Server 2008 或者 Windows Server 2003 SP1/SP2/R2 操作系统的网络服务器。大规模应用安全策略之前必须经过严格测试，确认可行之后方可部署。应用安全配置策略之后，必须重新启动计算机才生效。应用安全策略的主要操作步骤如下：

01 选择“开始”→“管理工具”→“安全配置向导”命令，打开“安全配置向导”对话框，单击“下一步”按钮，在“配置操作”对话框中，选中“应用现有安全策略”单选按钮，在“现有安全策略文件”文本框中单击“浏览”按钮，选择安全策略文件的路径，如图 1.16 所示。

02 单击“下一步”按钮，显示如图 1.17 所示“选择服务器”对话框，在“服务器”文本框中，输入想要应用到的服务器名称或 IP 地址。如果目标服务器为远程主机，则应单击“指定用户帐户”按钮，选择连接到指定主机部署安全策略使用的用户帐户及凭证。



图 1.16 “配置操作”对话框

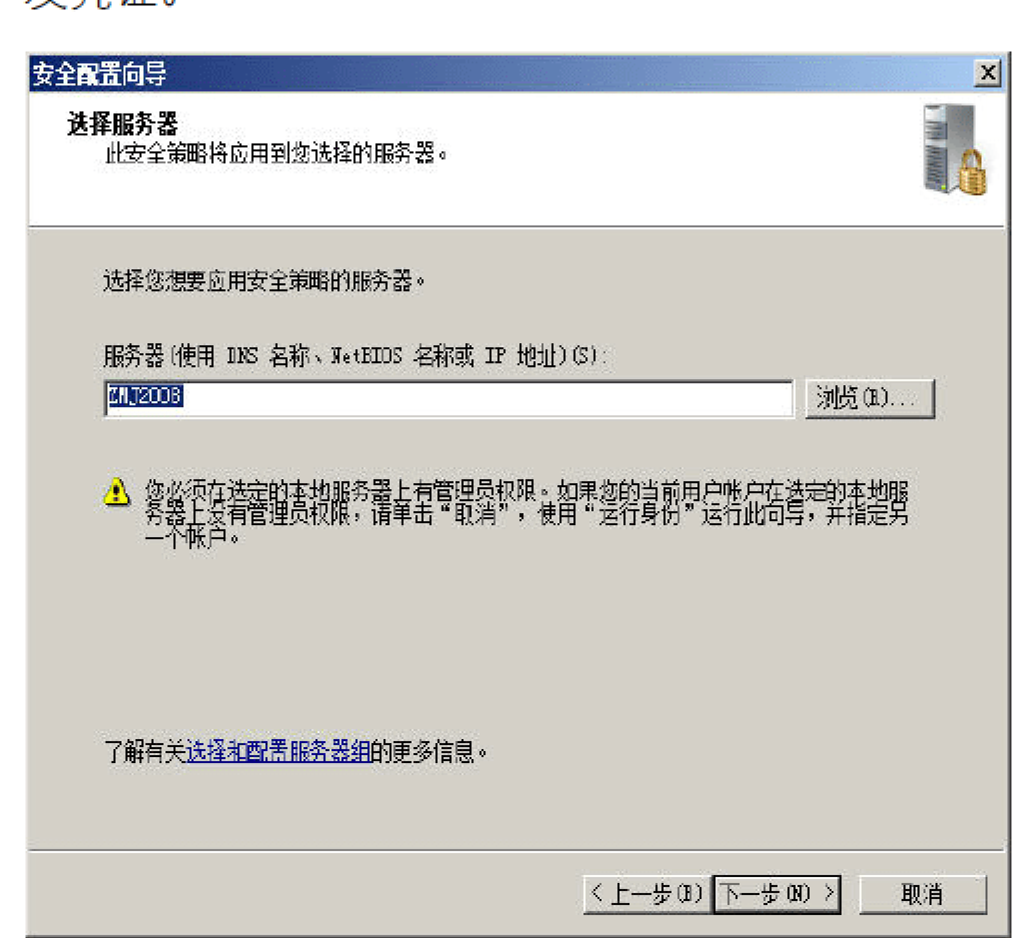


图 1.17 “选择服务器”对话框

03 依次单击“下一步”按钮，查看安全策略内容并应用，如图 1.18 所示。在“应用安全策略”对话框中，可以查看所选安全策略的描述信息，单击“查看安全策略”按钮打开“SCW 查看器”窗口，查看其详细信息。将安



全策略应用到本地计算机大概需要几分钟时间，应用到远程计算机时所需时间可能更长一些。

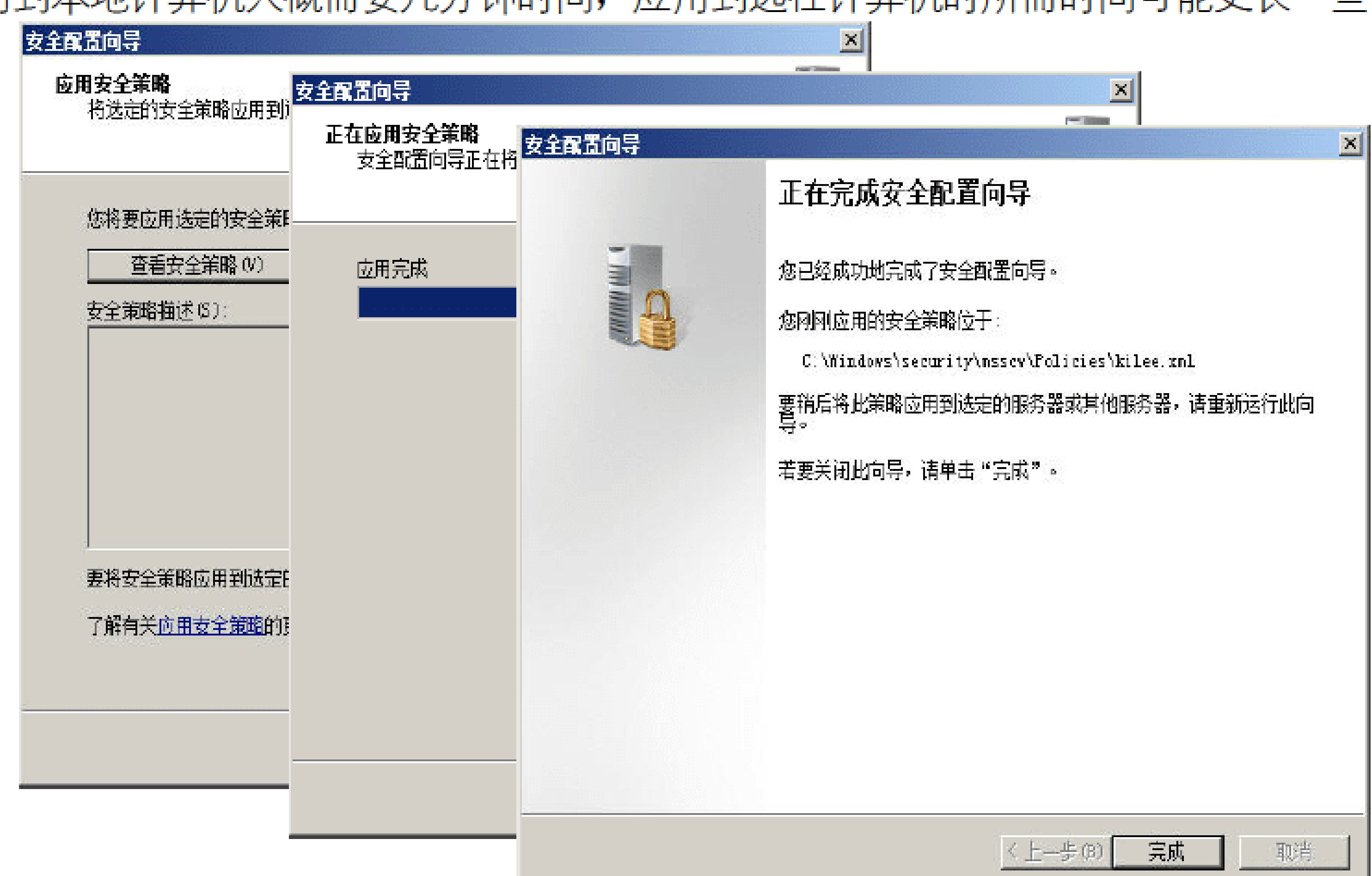


图 1.18　查看安全策略内容并应用

04 单击“完成”按钮，关闭安全配置向导。重新启动计算机后，应用的安全策略即可生效。

1.3.2　配置 Windows Defender

间谍软件通常是指自动安装，或者未提供足够通知、同意或控制的情况下，就在计算机上运行的应用程序。为了应对网络中泛滥的木马、间谍软件等恶意程序对系统安全的挑战，微软也推出了反木马、间谍软件的专用程序 Windows Defender。Windows Defender 的前身是 Giant 公司的 Giant Antispyware，微软将该公司收购后将其更名为 Windows Defender。

1. Windows Defender 概述

Windows Defender 是微软公司提供的一款免费组件，并且在 Windows Vista 和 Windows Server 2008 系统中，Windows Defender 已经成为系统默认安装的安全组件之一。Windows Defender 具有如下主要功能。

（1）提供完备的恶意软件清除功能

Windows Defender 在扫描查杀的同时，还会对恶意软件添加的文件以及修改的注册表内容进行同步检测和删除，清除比较干净。

（2）与杀毒软件相得益彰

Windows Defender 是设计用来检测、删除或隔离用户电脑中的已知或可疑间谍软件的安全防御工具，针对的是杀毒工具无法处理的恶意软件，所以并不会和系统中安装的防病毒软件冲突，相反两者配合工作，安全防御效果会更好。

（3）提供多种灵活扫描方式

Windows Defender 提供如下 3 种扫描方式，用户可根据实际需要选择：

- Quick Scan：它可以扫描间谍软件常用的安装目录，可以在最短的时间里发现大多数间谍软件；
- Full Scan：它可以扫描电脑中的全部硬盘分区以及全部文件夹。这种扫描方式非常彻底，但是耗时较多，具体的耗时根据用户的硬盘大小以及文件多少来决定。另外，扫描过程中，系统的整体运行速度会有所下降；
- Custom scan：在这种方式下，用户可以选择所要扫描的硬盘分区和文件夹。如果 Windows Defender 在这种模式下发现了间谍软件，将进而启动 Quick Scan 模式对间谍软件进行清除或隔离。

（4）实时监控功能

Windows Defender 最大的特点在于当恶意软件试图入侵计算机时，会自动提醒用户。需要注意的是，只有当恶意软件是与其它软件捆绑安装时，Windows Defender 才会警报提醒，而当直接安装恶意软件时，则不会表现任何动作。

（5）管理员可以监控用户行为

管理员可以允许用户使用 Windows Defender 扫描电脑，在发现可疑程序后选择相应的执行动作，以及查看 Windows Defender 的活动纪录。管理员还可以限制 Windows Defender 的管理权限。在默认情况下，任何用户都可以使用 Windows Defender。

2. 配置 Windows Defender 选项

如果不希望每次使用 Windows Defender 的默认设置扫描系统，可以在“Windows Defender”窗口中，单击“工具”按钮进行自定义配置，打开“工具和设置”对话框，继续单击“选项”链接，打开如图 1.19 所示窗口，在这里即可设置包括计划扫描、实时防护、默认操作、管理员选项等在内的 Windows Defender 高级选项。

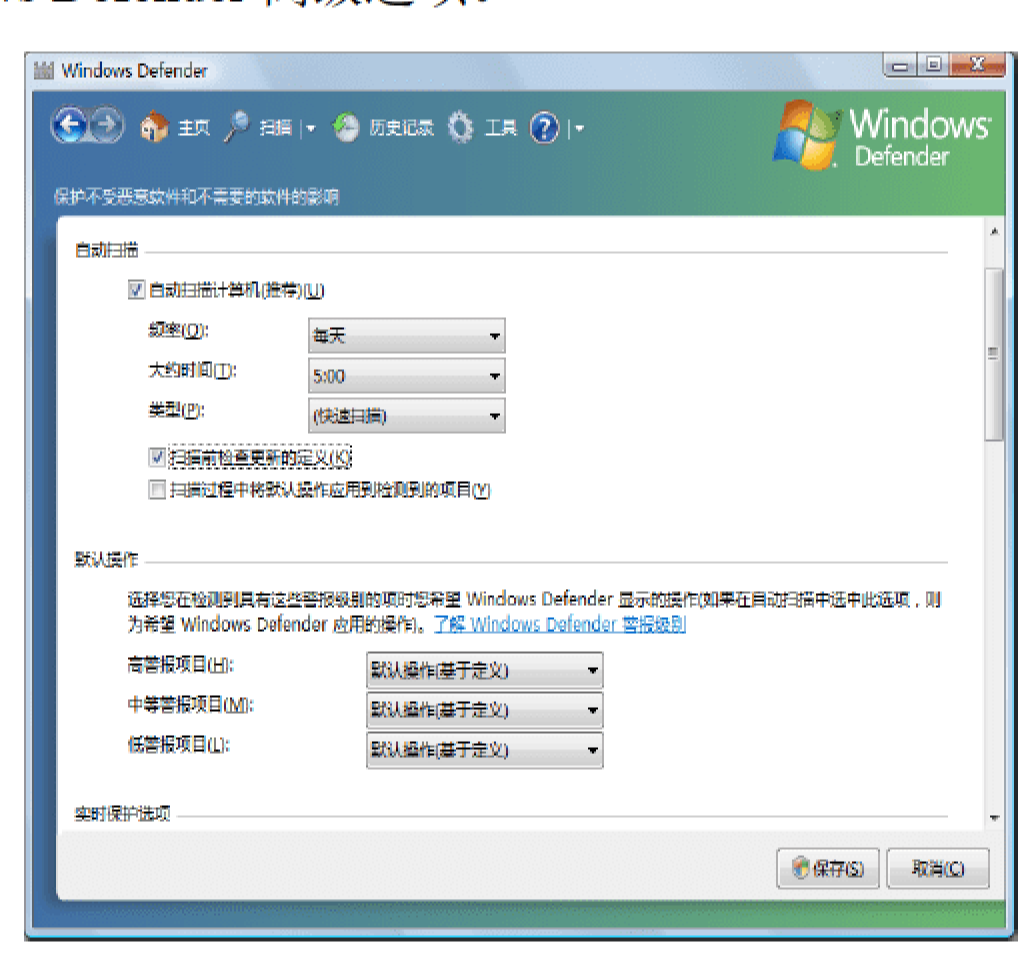


图 1.19　配置 Windows Defender 选项

（1）自动扫描

在“自动扫描”选项区域，选中“自动扫描计算机”复选框，然后设置适当的扫描频率（如



每天，每周等）和执行扫描的时间，并在“类型”下拉列表中选择希望执行的扫描方式即可。建议选中“扫描前检查更新的定义”复选框，以便确保 Windows Defender 定义库的最新状态。

（2）默认操作

在“默认操作”选项区域中，可设置在不同警报级别下所执行的操作。Windows Defender 默认提供 3 种警报等级，分别为：高警报项目、中等警报项目和低警报项目。用户可以根据需要为每一种警报等级的项目设置不同的操作，如对于扫描过程中发现的“高警报项目”，可以直接将默认操作定义为“删除”，对于低警报项目则可以设置为“忽略”。

- 高警报项目。可能搜集个人信息并对您的隐私产生负面影响或损害计算机的程序，例如，通常在未经用户允许的情况下，搜集信息或更改设置。建议立即删除此类项目；
- 中等警报项目。可能影响用户的隐私或更改计算机对计算体验产生负面影响的程序，例如，搜集个人信息或更改设置。对于此类项目，建议用户复查警报详细信息，查看为何会检测到此软件。如果不喜欢软件的操作方式，或如果不了解和信任发行者，则考虑阻止或删除此类项目；
- 低警报项目。可能不需要的软件会搜集有关用户或计算机的信息，或更改计算机的运行方式，但它按照协议操作，安装时会显示许可条款。此类项目应视情况而定，如果安装之前提示相关信息及安装结果，则可以保留。如果不能确定信任该软件的发行者，则建议删除。

（3）实时保护选项

在如图 1.20 所示“实时保护选项”区域中，选中“使用实时保护”复选框，即可启用 Windows Defender 实时保护功能。Windows Defender 实时保护的项目包括：系统配置、IE 加载项、Internet Explorer 配置、服务和驱动、应用程序执行、应用程序注册、Windows 加载项等。默认情况下，Windows Defender 已经对所有安全代理组件开启实时保护功能。

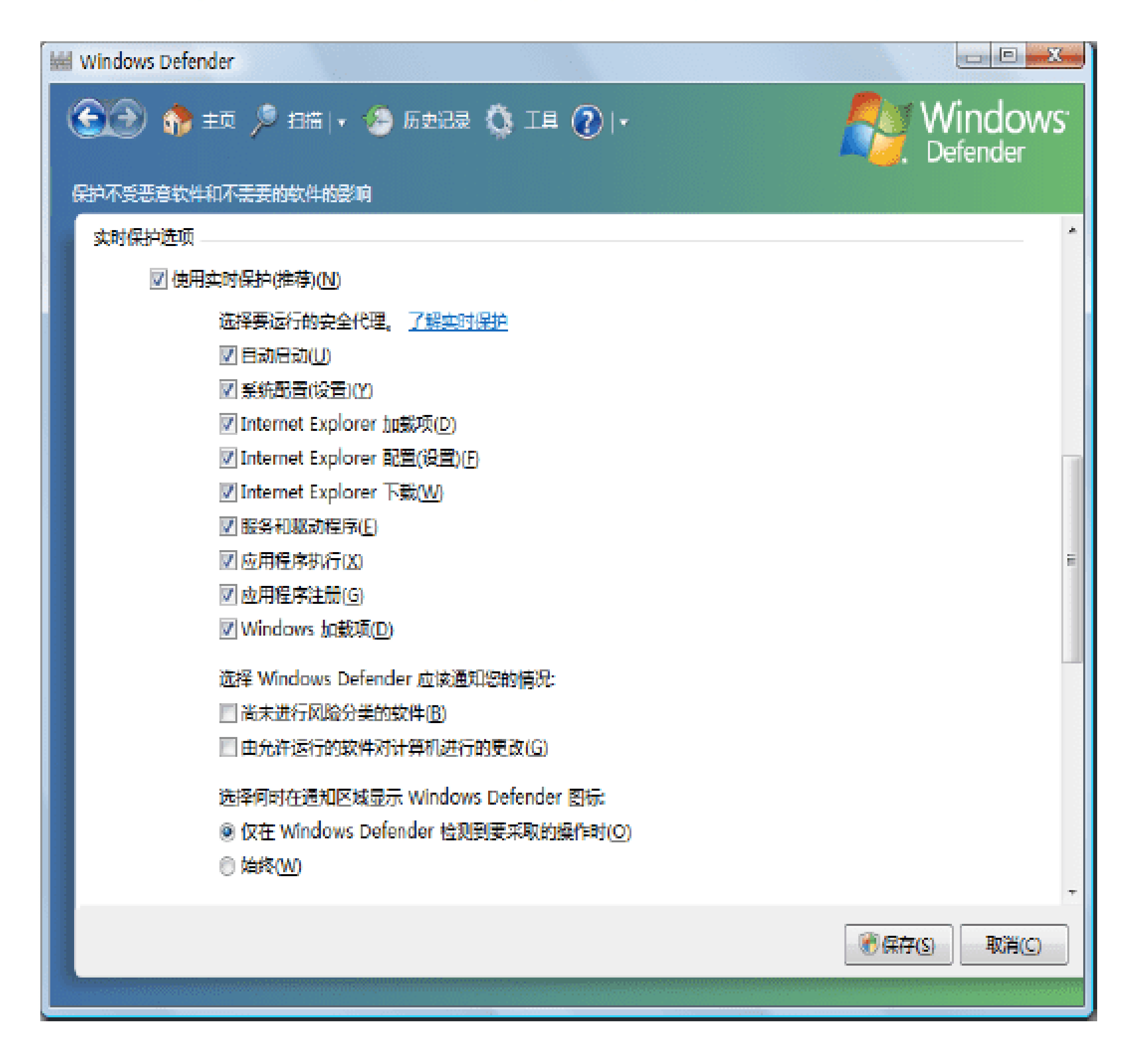


图 1.20　实时保护选项

（4）高级选项

在如图 1.21 所示“高级选项”选项区域中，用户可以对 Windows Defender 扫描时的如下

4 个高级选项进行设置：

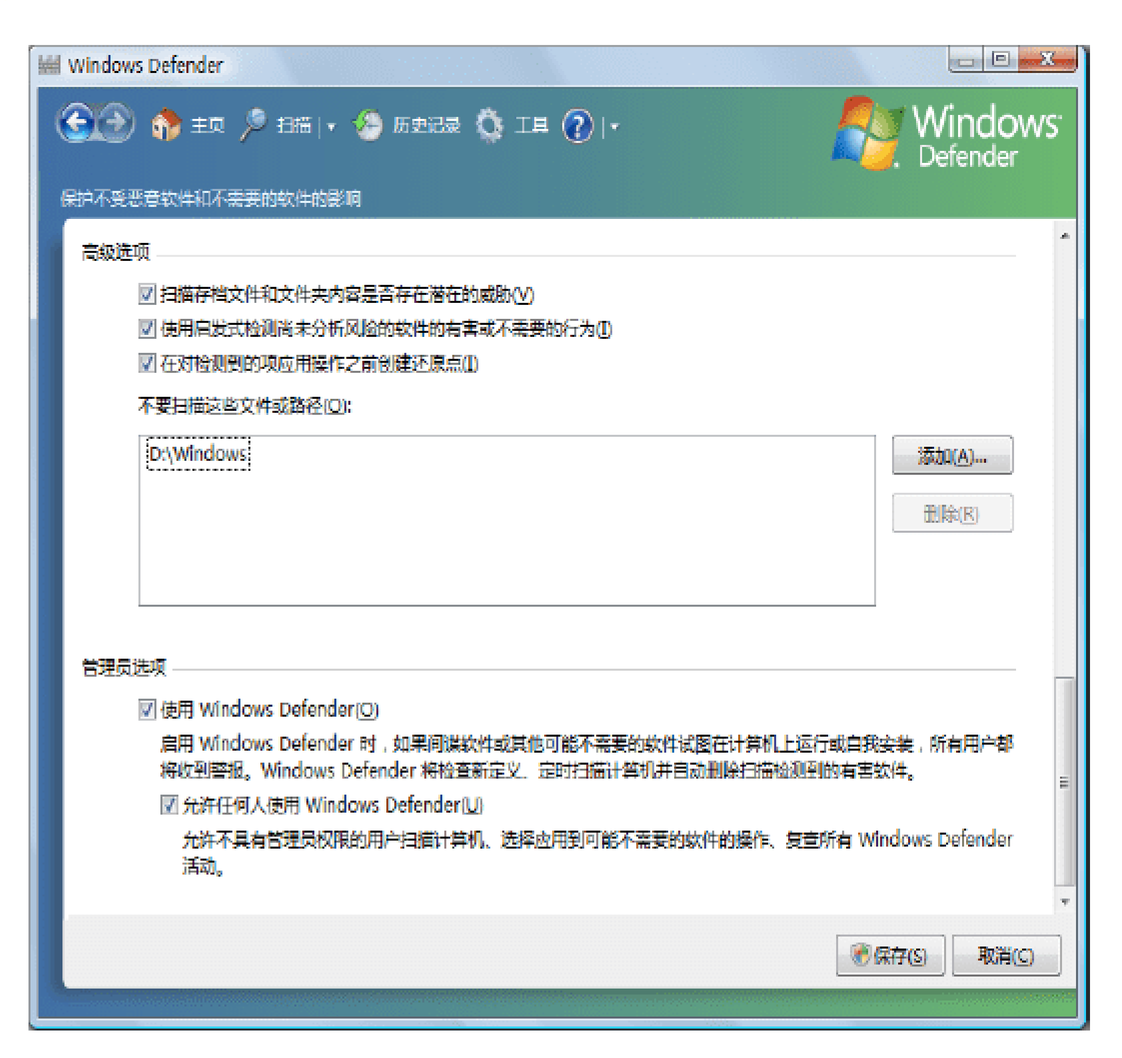


图 1.21　高级选项

- 扫描存档文件和文件夹的内容是否存在潜在的威胁。扫描这些位置可能会延长扫描时间，但间谍软件和其他可能不需要的软件会自行安装并试图“隐藏”在这些位置中；
- 使用启发式检测尚未分析风险的软件的有害或不需要的行为。Windows Defender 使用定义文件识别已知威胁，但它还可以检测未在定义文件中列出的软件的可能有害或不需要的行为，并向用户发出警报；
- 在对检测到的项目应用操作之前创建还原点。由于可以将 Windows Defender 设置为自动删除检测到的项目，因此如果要使用原本不想删除的软件，则可以选择此选项还原系统设置；
- 不要扫描这些文件或路径。使用此选项可以选择任何用户不希望 Windows Defender 扫描的文件和文件夹。

（5）管理员选项

在“管理员选项”区域中，选中“使用 Windows Defender”复选框，当间谍软件或其他潜在不安全的软件试图运行或安装在计算机上时，用户将收到 Windows Defender 发出的警报；若选中“允许任何人使用 Windows Defender”复选框，则允许没有管理员权限的用户使用 Windows Defender。

3. 更新 Windows Defender 定义库

使用 Windows Defender 时，保持其定义库处于最新状态是非常重要的。定义是一些文件，其中包含了已知间谍软件和其他可能不需要的软件特称代码，类似于防病毒程序的病毒库。由于间谍软件在不断发展，Windows Defender 依靠更新定义来确定正尝试在计算机上安装、运行或更改设置的软件是否为可能不需要的或恶意软件。

在配置 Windows Defender 自动扫描时，如果选中“扫描前检查更新的定义”复选框，即可将其配置为自动更新定义。除此之外，用户还可以通过手动方式更新 Windows Defender 定义库。在“Windows Defender”窗口中，单击“帮助”按钮旁边的箭头，并选择“检查更新”



即可。为确保计算机安全，Windows Defender 会在定义文件过期超过七天未更新时通知用户，此时直接单击“立即检查更新”按钮即可，如图 1.22 所示。

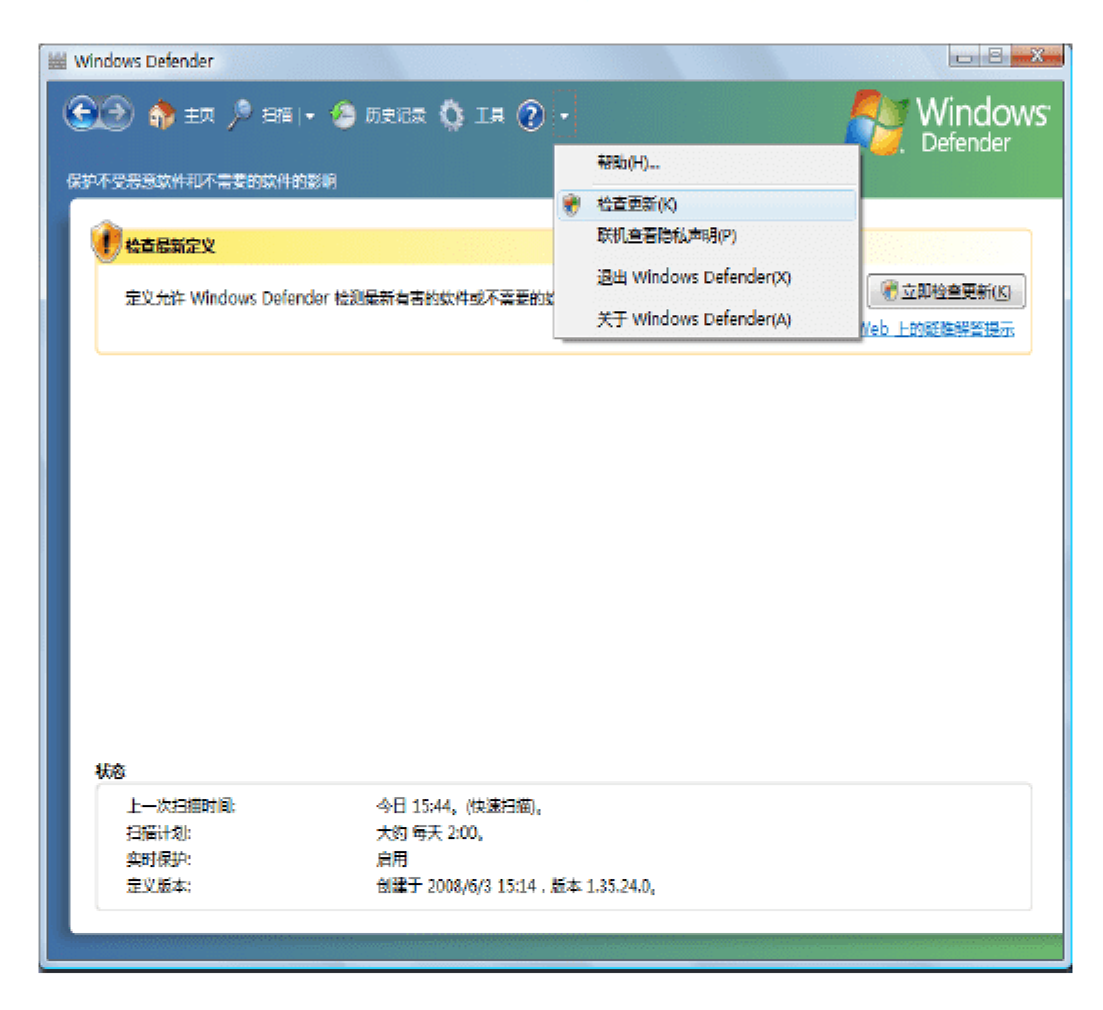


图 1.22　更新 Windows Defender

4. 注意事项

默认情况下，服务器系统都是使用最小方式安装的，所以 Windows Defender 组件不会出现在控制面板中。管理员可以通过“管理服务器”控制台，启动“添加功能向导”，在“选择功能”列表中，选中“桌面体验”组件并安装，如图 1.23 所示。安装完成后即可配置和使用 Windows Defender。

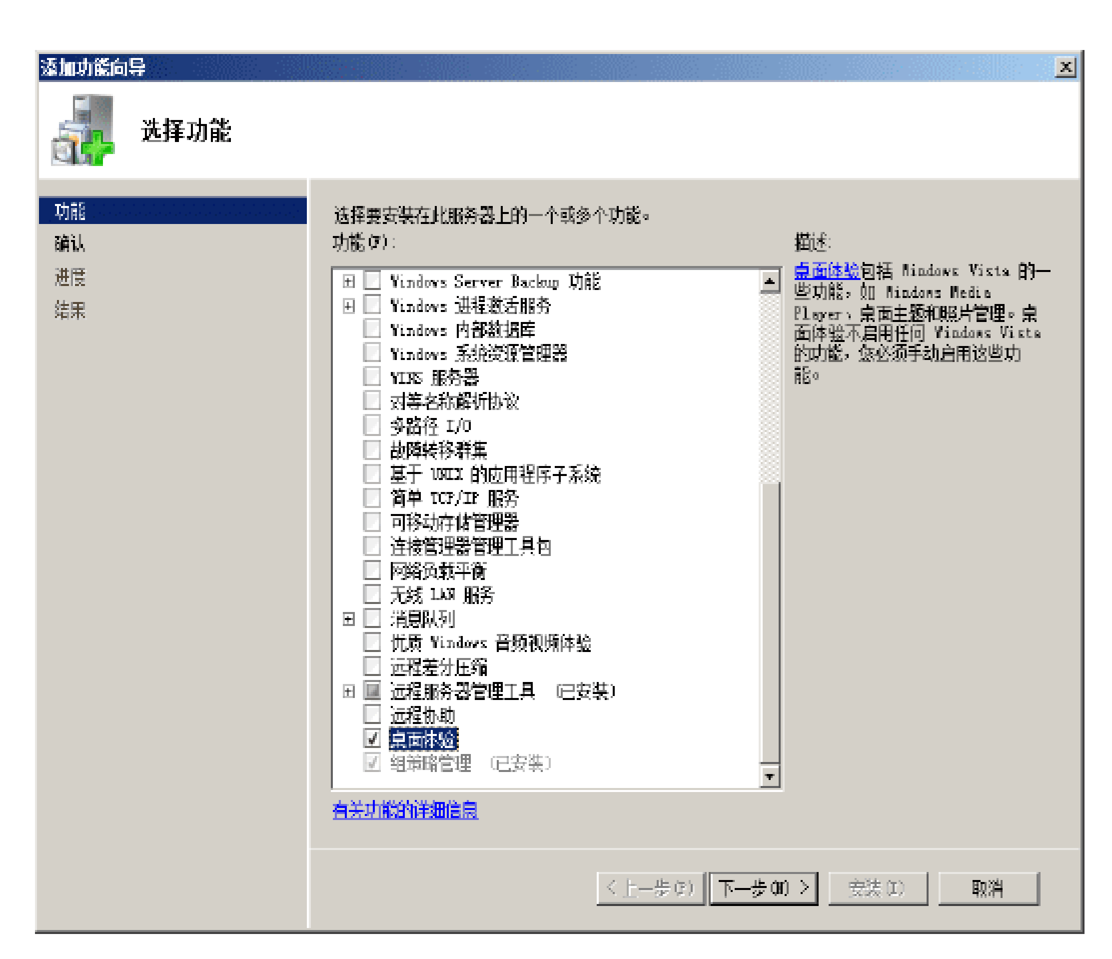


图 1.23　“选择功能”对话框

1.3.3　注册表安全

注册表中包含了 Windows 系统运行时所需的信息，例如，每个用户的配置文件、计算机上安装的应用程序及其设置、系统上存在哪些硬件以及正在使用哪些端口等。因此，注册表作为 Windows 系统中重要的配置文件，对系统安全起着决定性的作用。

1. 禁止注册表远程访问

Windows Server 2008 在默认安装时启用了允许远程访问注册表。需要注意的是，系统服务的启动、ACL 权限的修改、用户名的建立等信息，都可以在注册表中完成，因此开启此功能将会对系统安全带来极大的隐患，必须严格禁止使用远程注册表访问功能。该安全设置确定在网络上可访问哪些注册表路径和子路径，无论注册表项 winreg 的访问控制列表中列出的是用户还是组。

01 打开组策略控制台，依次展开“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“安全选项”，显示如图 1.24 所示窗口。

02 在右侧的策略窗口中，双击“网络访问：可远程访问的注册表路径和子路径”策略，显示如图 1.25 所示“网络访问：可远程访问的注册表路径和子路径 属性”对话框。删除列表框的所有数据，最后单击“确定”按钮即可。

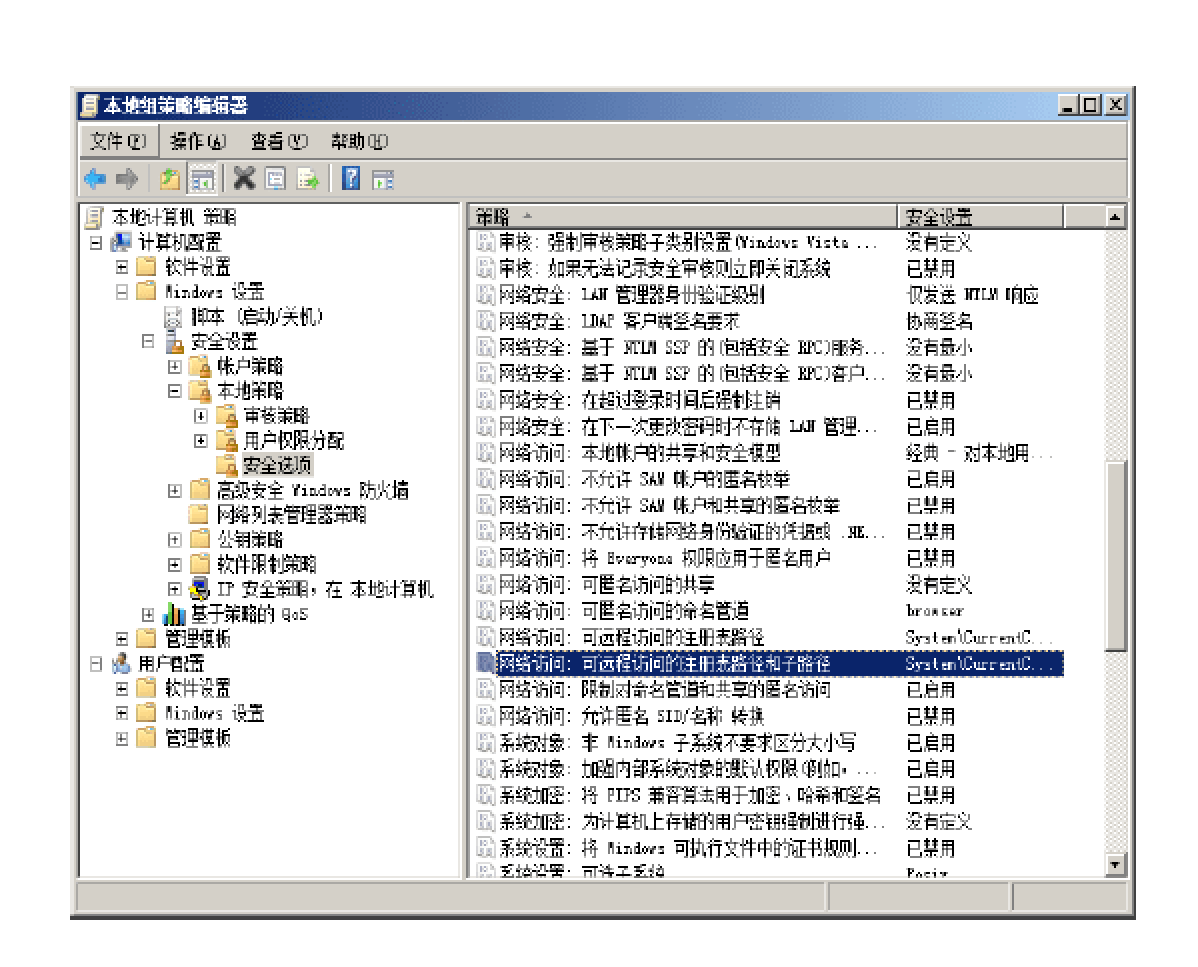


图 1.24 “本地组策略编辑器”窗口

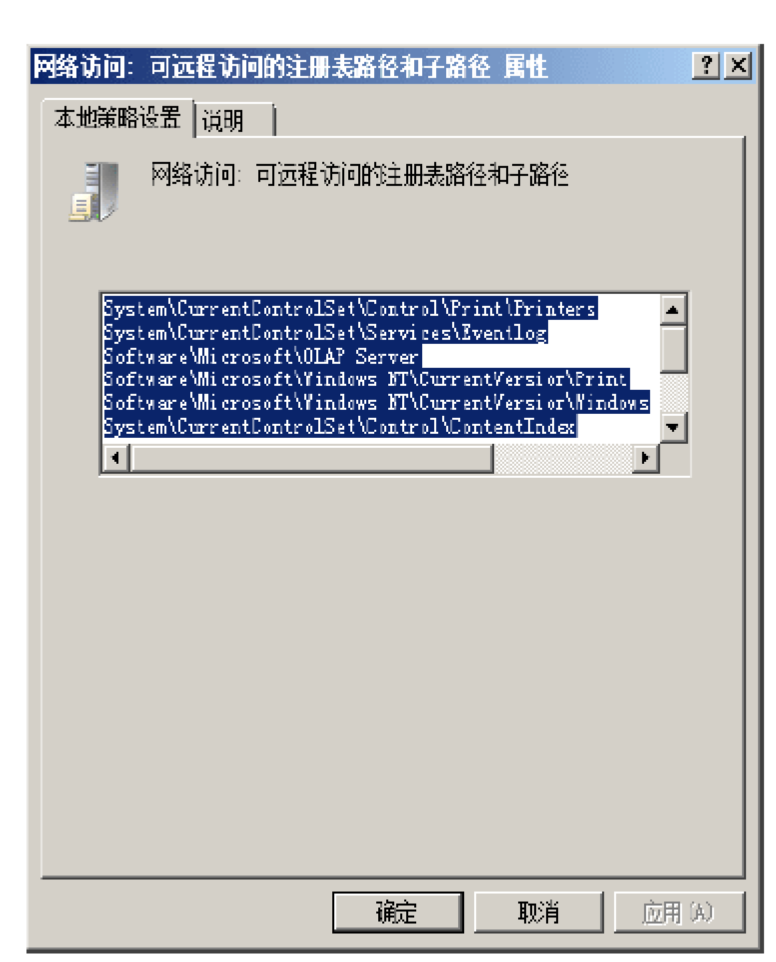


图 1.25 “网络访问：可远程访问的注册表路径和子路发属性”对话框

03 双击“网络访问：可远程访问的注册表路径”策略，显示如图 1.26 所示“网络访问：可远程访问的注册表路径属性”对话框。

04 删除文本框的所有数据，然后单击“确定”按钮即可。



提示 编辑注册表不当可能会严重损坏系统。在更改注册表之前，应备份计算机上任何有价值的数据。

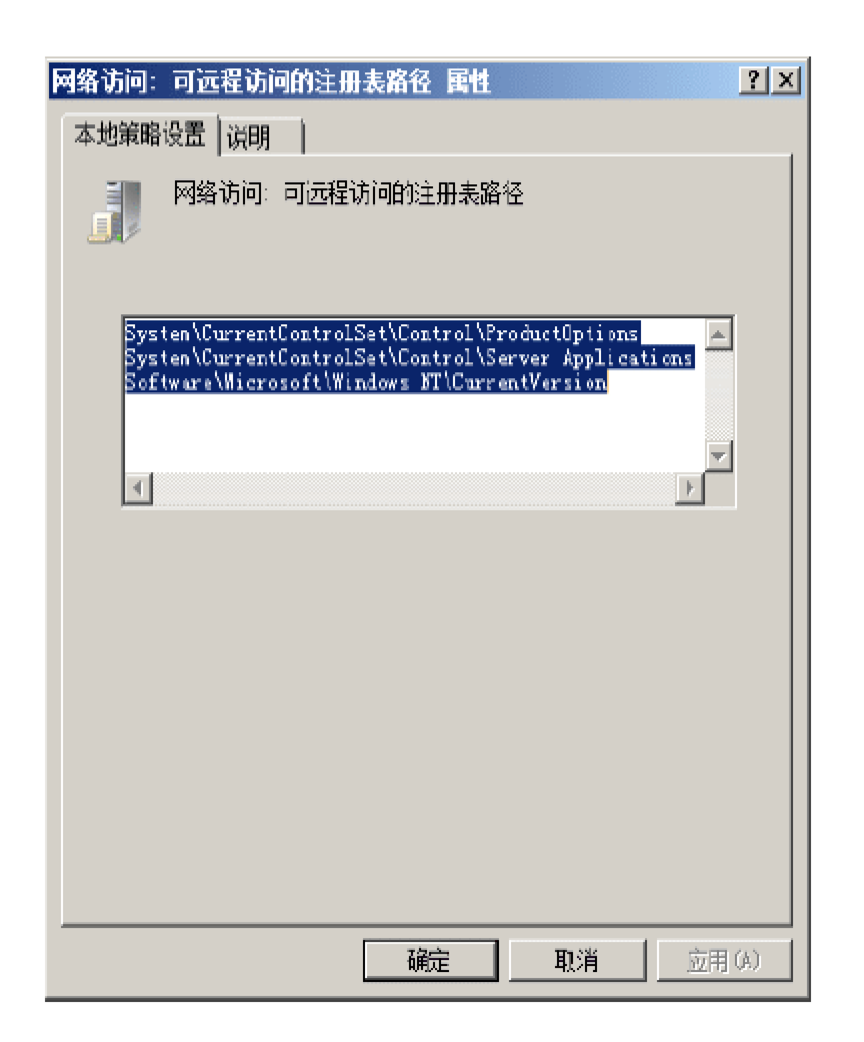


图 1.26 “网络访问：可远程访问的注册表路径 属性”对话框



2. 注册表安全设置

Windows Server 2008 系统注册表中常用的安全设置包括如下几项。

（1）隐藏重要文件/目录可以修改注册表实现完全隐藏

在注册表项 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current-Version\Explorer\Advanced\Folder\Hi-dden\SHOWALL 中，右击 “CheckedValue”，选择快捷菜单中的“修改”选项，把数值由 1 改为 0。

（2）对匿名连接的额外限制

没有显示的匿名权限就没有办法访问，在注册表 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa 下修改“restrictanonymous”为 2。

（3）关闭默认的根目录和管理共享

去除 Windows 安装后生成的默认共享。在注册表 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Lanmanserver\Parameters 添加 DWORD 值 autosharews 为 0 ，以及 autoshareserver 为 0。

（4）禁止 Guest 用户访问日志

取消来宾账号机器同组账号访问日志的权利。分别将在 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog 下 3 个子键 Application、Security、System 下面的 RestrictGuestAccess 值该为 1 即可。

（5）禁止显示上次登录的用户名

防止在登录界面上泄漏账号信息。在注册表 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon 下面修改 Dontdisplaylastusername 为 1 即可。

（6）禁用文件名创建

取消 Windows Server 2008 和 Windows Server 2003 为兼容以前微软文件名命名方式带来的性能损失。在注册表 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem 下面设置 Ntfsdisable8dot3namecreation 为 1 即可。

（7）禁用无用的子系统

取消因为使用例如 dos、win16、os/2、posix、应用系统下的程序子系统可能带来的隐患。

- 修改 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SessionManager\Subsystems 键下的 Optional 的值为 “0000”;
- 删除同一子键下的 os2、posix 项，同时删除 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\wow 下的子键;
- 删除 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SessionManager\environment 下的 OS2libpath 项;

■ 删除 HKEY_LOCAL_MACHINE\Software\Microsoft\os/2 Subsystem for nt 下的所有子键。

（8）不支持 IGMP 协议

在注册表 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters 的子项下，新建 DWORD 值，名为 IGMPLevel 值为 0 即可。

（9）防止 ICMP 重定向报文的攻击

在注册表 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters 的子项下，将 EnableICMPRedirects 值设为 0 即可。

（10）修改终端服务端口

在注册表的第一处位置，在 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer\Wds\rdpwd\Tds\tcp 的子项下，在右边的 PortNumber 键值下，在十进制状态下改成需要变更的端口号只要不与其他冲突即可。

第二处位置，在 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp 方法同上，需要注意的是，设置的端口号必须与前面的值相同。

（11）保护系统不守一定的拒绝服务攻击

防备 SYN 泛滥攻击，在 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\parameters 键下分别添加：

■ DWORD 值 SynAttackprotect 为 2；
■ Tcpmaxhalfopen 值为 100；
■ Tcpmaxhalfopenedretried 的值为 80；
■ Tcpmaxportsexhausted 的值为 5。

（12）加强防备拒绝服务攻击

终止半开放的 TCP 连接，可在上面同一键下添加 Tcpmaxconnectreponseretransmissions 为 3。

（13）TCP 空连接计数器

可以防止死连接消耗资源，可以尽快结束死连接，在 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\parameters 键下添加 DWORD 值 Keepalivetime 为 300000，该计算单位为毫秒，即 5 分钟。

（14）不轻易改变 MTU 的值（最大传输单元）

防止 Windows Server 2008 和 Windows Server 2003 自动执行的 MTU 探索被恶意用户利用导致系统采用极小 MTU 值从而增强资源消耗的拒绝服务攻击，可在同一键值下面添加 DWORD 值 Enablepmtudicovery 为 0。

（15）禁用 IP 路由

防止恶意用户利用非法覆盖正常路由选择，应该在 HKEY_LOCAL_MACHINE\System\



CurrentControlSet\Services\Tcpip\parameters 键下添加 DWORD 值 DisableIPsourcerouting 为 2。

（16）禁用 ICMP 转向

防止恶意用户利用来改变 Windows Server 2008 Windows Server 2003 或路由表以响应网络设备发送给它的 ICMP 重定向消息，应该在 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\parameters 键下修改 EnableICMPredirect 值为 0。

（17）禁止光盘自动启动

防止恶意用户利用此手段访问系统，在 HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer 下设置“Nodrivetypeautorun”为 149。该设置仅适用于 Windows XP\Vista\2003，不适用于 Windows Server 2008 系统。

（18）只有本地用户才可以访问软盘

防止恶意用户利用此方法访问系统，修改 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon 下的“allocatefloppyes”值为 1。

（19）只有本地登录的用户才能访问 CDROM

防止恶意用户利用此手段访问系统，修改同一键下的“allocatecdroms”值为 1。

（20）在关机时清理虚拟内存页面交换文件

防止虚拟内存页面交换文件泄漏可用的信息，修改 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SessionManager\Memory management 键下的“clearpagefileatshutdown”值为 1。

1.3.4　实现系统服务安全

任何网络服务的安装的提供都是建立在系统服务的基础上的，因此做好系统服务安全是系统安全和网络安全的重要环节。任何服务都可能存在漏洞，但也不能“因噎废食”，最佳方案就是通过一切可行方法，确保系统服务的安全，如禁用非必要服务、设置服务访问权限等。

1. 系统服务配置注意事项

配置系统服务时应注意以下事项：

- 根据服务的描述以及业务的需求，确定是否使用此服务；
- 具体每个服务的内容和功能，请参考微软的说明和咨询业内安全专家；
- 禁止或者设置成手动启动的方式处理系统非必须的服务；
- 如对系统可能造成的影响不了解，在测试环境中测试验证通过以后，再在应用环境中部署；
- 对于安装应用程序同步安装的服务，如无必要，应将其关闭。

依次选择“开始”→“管理工具”→“服务”命令，打开“服务”控制台窗口，显示本地计算机中所有的服务，显示如图 1.27 所示结果。

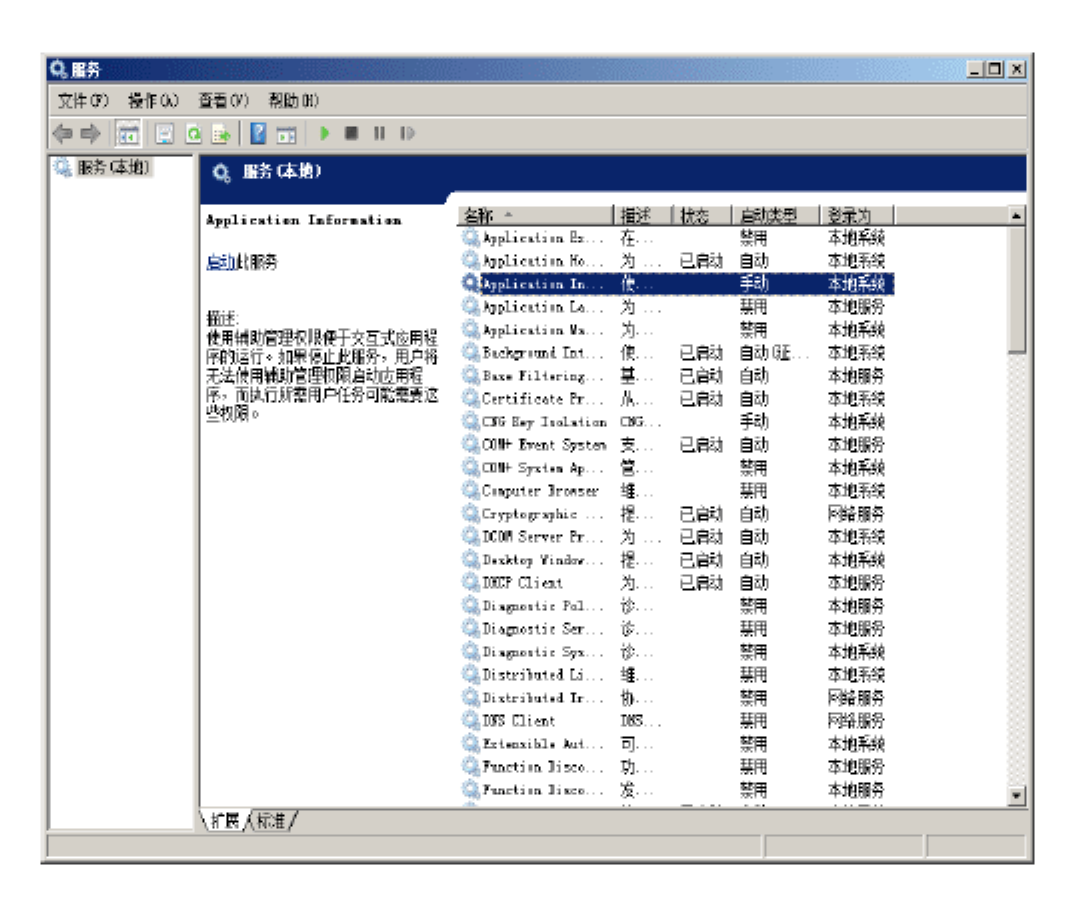


图 1.27　默认安装的服务列表

系统服务的处理不同于其他设置，因为所有服务的漏洞、对策及潜在影响在本质上都一样。安装 Windows Server 2008 操作系统时，系统将在启动时创建并配置默认服务。有些服务在组织环境中并不需要，但仍在 Windows 中被启用，来确保应用程序或客户端兼容或辅助进行系统管理。



提示　Windows Server 2008 系统中的“服务”管理工具，与 Windows Server 2003 系统基本相同。

2. 服务

服务仅在登录到某一帐户的情况下才能访问操作系统中的资源和对象。大多数的服务都不更改默认的登录帐户，更改默认帐户可能导致服务失败。如果选定帐户没有登录计算机服务的权限，Microsoft 管理控制台的服务管理单元将自动为该帐户授予登录服务的用户权限，但并不一定会启动服务。Windows Server 2008 与 Windows Server 2003 相同，系统包括 3 个内置的本地帐户，分别用作各系统服务的登录帐户。

（1）本地系统帐户

本地系统帐户功能强大，它可对本地系统进行完全访问，并为网络中的计算机提供服务。有些服务的默认配置使用的是“本地系统”帐户，则不需要更改默认服务设置。本地系统帐户名称是 LocalSystem，没有密码设置。

（2）本地服务帐户

本地服务帐户是一种特殊的内置帐户，类似于经过身份验证的用户帐户。就访问的资源的对象而言，“本地服务”帐户与“Users”组成员权限等同。这种限制性访问有助于在个别服务或进程受损时保障系统安全，以“本地服务”帐户运行的服务使用有匿名凭据的空会话来访问网络资源。帐户名称为 NTAUTHORITY\LocalService，该帐户没有密码。

（3）网络服务帐户

网络服务帐户也是一种特殊的内置帐户，类似于经身份验证的用户帐户。就访问的资源的对象而言，“网络服务”帐户与“Users”组成员权限等同。这种限制性访问有助于在个别服务或进程受损时保障系统安全，以“网络服务”帐户运行的服务可使用计算机帐户的凭据来访问网络资源。帐户名称为 NTAUTHORITY\NetworkService，该帐户没有密码。



注意 如果更改默认服务设置，重要的服务可能无法正常运行。最重要的是，更改启动类型一定要谨慎，要使用配置了自动启动服务的设置来登录。

3. 漏洞

任何服务或应用程序都是潜在的攻击点，因此，必须禁用或删除系统环境中不需要的服务或可执行文件，或者直接删除闲置的网络服务。

注意 

如果启用附加服务，则会因依赖关系而要求同时启动其他服务。首先明确在组织中执行任务的服务器角色，然后将特定服务器角色所必需的所有服务添加到策略中。

4. 对策

系统服务中的“策略”可以有以下 4 种设置方式：

- 自动；
- 手动；
- 禁用；
- 未定义。

对于所有不必要的服务应当禁用。此外，还可通过配置用户定义帐户列表的访问控制列表（ACL），编辑服务安全性。

5. 潜在影响

虽然禁用不必要的服务可以减少系统资源的占用以及系统漏洞，但有些服务（如 Security Accounts Manager）禁用后将导致系统无法引导，禁用一些关键服务可能使计算机无法通过域控制器的身份验证。因此，为安全起见，在禁用系统服务前应先在测试环境中测试。

注意 

管理员还可以选择“计算机配置”→“Windows 设置”→“安全设置”→“系统服务”选项，在打开的“组策略对象编辑器”中配置“系统服务”设置。

小　　结

Windows Server 2008 在安装配置过程中用户需注意安全性和易用性之间的矛盾，根据实际需求设置适当的安全级别即可。在安装过程中，无需设置计算机名、网络连接等信息，只要在安装完成后进行初始配置即可。在不同的使用环境下，Windows Server 2008 系统表现出来的安全防范能力是不一样的，甚至该系统在某些方面没有一点安全抵抗能力，这就需要手动来保护 Windows Server 2008 系统的运行安全。

习　　题

1. Windows Server 2008 有哪些版本？
2. 与以前的版本相比，Windows Server 2008 有哪些新特性？
3. 在安装 Windows Server 2008 前要作什么准备？
4. 如何对 Windows Server 2008 进行初始配置？
5. 如何对 Windows Server 2008 进行安全配置？

实验：Windows Server 2008 基本安全配置

实验目的

掌握 Windows Server 2008 的初始配置。

实验内容

为全新安装完成的 Windows Server 2008 系统，设置 IP 地址、主机名等基本信息，并启用 Windows 防火墙、自动更新和 Windows Defender。

实验步骤

1. 使用光盘安装 Windows Server 2008。
2. 设置 IP 地址和主机名。
3. 启用 Windows Update 和 Windows 防火墙。
4. 配置 Windows Defender，升级定义库并实施快速扫描。

第2章

Windows Server 2008用户环境安全设置

每个用户使用计算机的习惯有所不同，例如设置个性化桌面、系统主题等，当登录到其他计算机时，为了便于使用还需要再次进行设置，非常麻烦。另外，如果用户网络安全意识不高，不正确的系统设置还可能导致系统漏洞的产生。在 Windows 域网络中，管理员可以对用户帐户的配置文件进行设置，使用户在网络中任何计算机上登录时都可以自动下载到自己的配置文件，免去重新设置工作环境的操作。

本章导读

- 用户环境设置
- IE 浏览器安全设置

Windows Server 2008

2.1 用户环境设置

用户工作环境就是用户桌面上所出现的内容，包括桌面的设置、应用程序的设置、文件夹设置、磁盘配额设置等。Windows Server 2008 安装完成后，管理员需要重新对系统进行配置，从而提高系统的安全性和适用性。

2.1.1 用户配置文件设置

通过“用户配置文件”可以设置用户的工作环境，以便用户每次登录时，都可以有相同的工作环境，如相同的桌面设置、相同的网络连接和网络打印机等。只要拥有足够的操作权限，任何用户配置文件都是可以重新设置的。由于每一种类型的用户配置文件都有其特殊的适用环境，因此必须掌握不同用户文件的配置方法，才可以灵活运用于网络管理中，实现快速统一部署。

1. 用户配置文件的类型

根据用户配置文件应用工作环境的不同，可以分为如下几种类型：

- 本地用户配置文件　第一次登录到计算机时，将创建本地用户配置文件，并存储在计算机的本地硬盘上。对本地用户配置文件所做的任何更改都只是针对用户所在的计算机；
- 漫游用户配置文件　漫游用户配置文件由系统管理员创建，通常存储在服务器上。每次登录到网络上的任何一台计算机时，都可以使用该配置文件。对漫游用户配置文件所做的更改将在服务器上更新；
- 强制用户配置文件　此文件是用来为个人或整个用户组指定特殊设置的漫游配置文件。只有系统管理员才能更改强制用户配置文件；
- 临时用户配置文件　当因错误而无法加载用户配置文件时，所发布的临时配置文件。每次会话结束时会删除临时配置文件。当用户注销时，将丢失用户对其桌面设置和文件所做的更改。

2. 用户配置文件的内容

用户配置文件并不是单纯的某个文件，默认用户配置文件中的 NTuser.dat 文件包含了 Windows Server 2008 家族的配置设置。每个用户配置文件还要使用包含在 All Users 文件夹中的公用程序组。总体而言，用户配置文件由以下 3 部分组成：

- 用户配置文件文件夹；
- Ntuser.dat 文件；
- All Users 文件夹。



3. 查看本地用户配置文件

当用户第一次登录某台计算机时，系统会自动为这个用户在该计算机上创建一个“本地用户配置文件”。在运行支持多用户 Windows 操作系统的计算机上，往往包含多个本地用户配置文件。其实，本地用户配置文件都是由默认的用户配置文件复制而来的。当用户注销、关机或重启时，用户的任何设置更改都将存储到该用户的本地用户配置文件而不会影响到其他用户帐户的本地用户配置文件。

01 选择“开始”→“控制面板”→“系统”命令，打开如图 2.1 所示“系统控制面板”窗口。

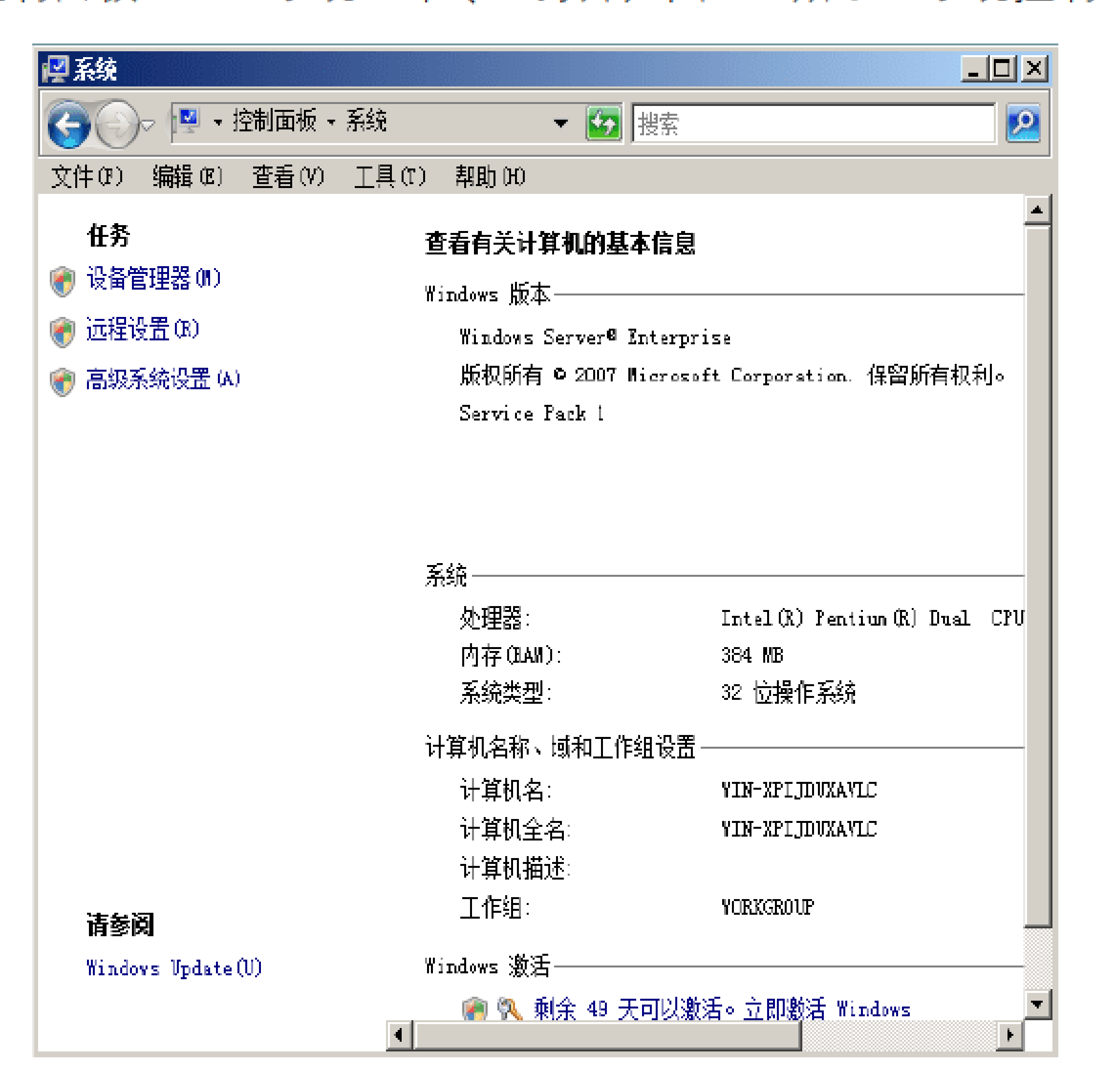
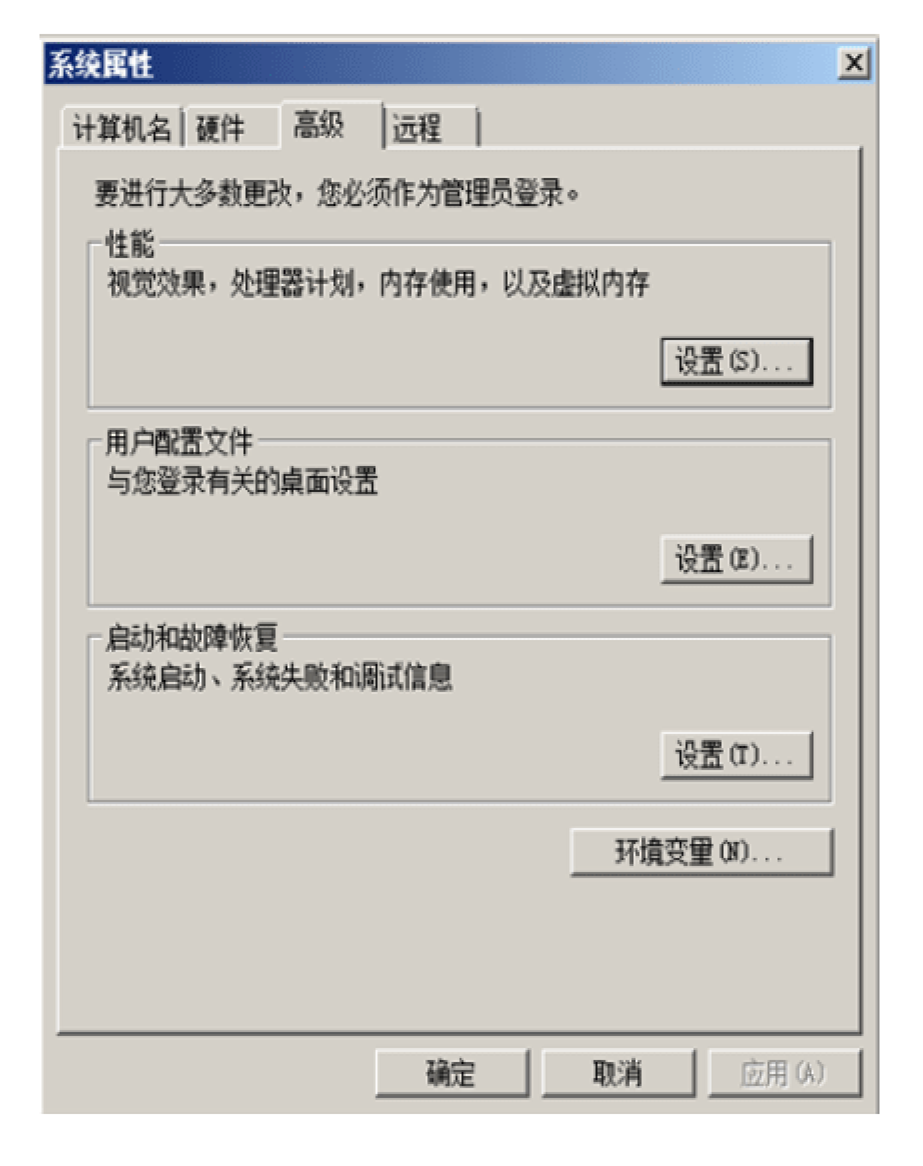


图 2.1　“系统控制面板”窗口

02 单击“高级系统设置”超链接，显示“系统属性”对话框。单击用户配置文件文本域中的“设置”按钮，显示如图 2.2 所示“用户配置文件”对话框，即可查看这台计算机内的用户配置文件。



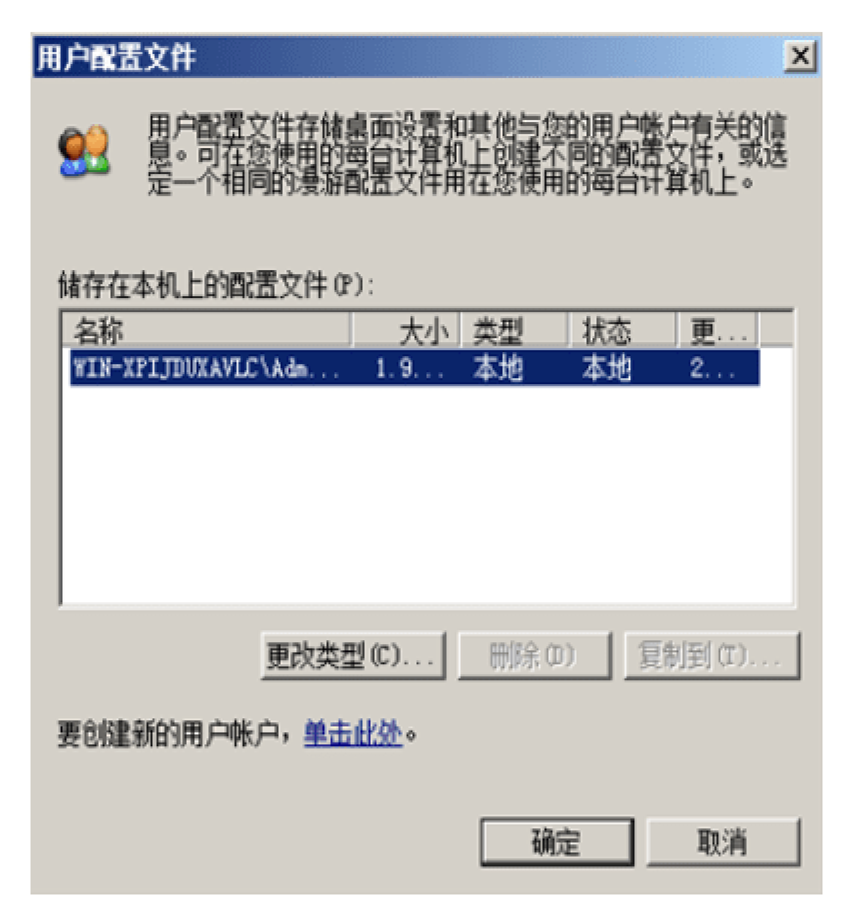


图 2.2　更改用户配置文件

4. 漫游用户配置文件

如果用户希望在网络上的任何一台计算机上登录时都使用相同的用户配置文件，即相同的工作环境，可以通过域控制器上的“漫游用户配置文件”来实现。当用户注销、关机或重启时，其环境的更改会自动存储到域控制器上的漫游用户配置文件内，因此用户再次登录时就会以这个更新过的用户配置文件为工作环境。

（1）设置漫游用户配置文件

设置漫游用户配置文件，首先要在域控制器上建立共享目录，然后在共享目下建立存放该漫游用户配置文件的文件夹。当该用户首次登录到域时，会在该文件夹内自动生成一个空的漫游用户配置文件。

01 以管理员权限的帐户登录到计算机，本地磁盘上新建一个文件夹，并命名为“company”。右击 company 文件夹，在快捷菜单中选择“共享”命令，显示“文件共享”对话框。在“选择要与其共享的网络上的用户”下拉列表中选择 Everyone 选项，单击“添加”按钮，并在“权限级别”下拉菜单中，将权限设置为“共有者”，显示如图 2.3 所示结果。单击“共享”按钮，完成共享文件夹设置。

02 选择“开始”→“管理工具”→“Active Directory 用户和计算机”命令，打开“Active Directory 用户和计算机”窗口。右击 Users 中的帐户 zhangsan，在快捷菜单中选择“属性”命令，打开如图 2.4 所示“zhangsan 属性”对话框。



图 2.3 “权限设置”对话框

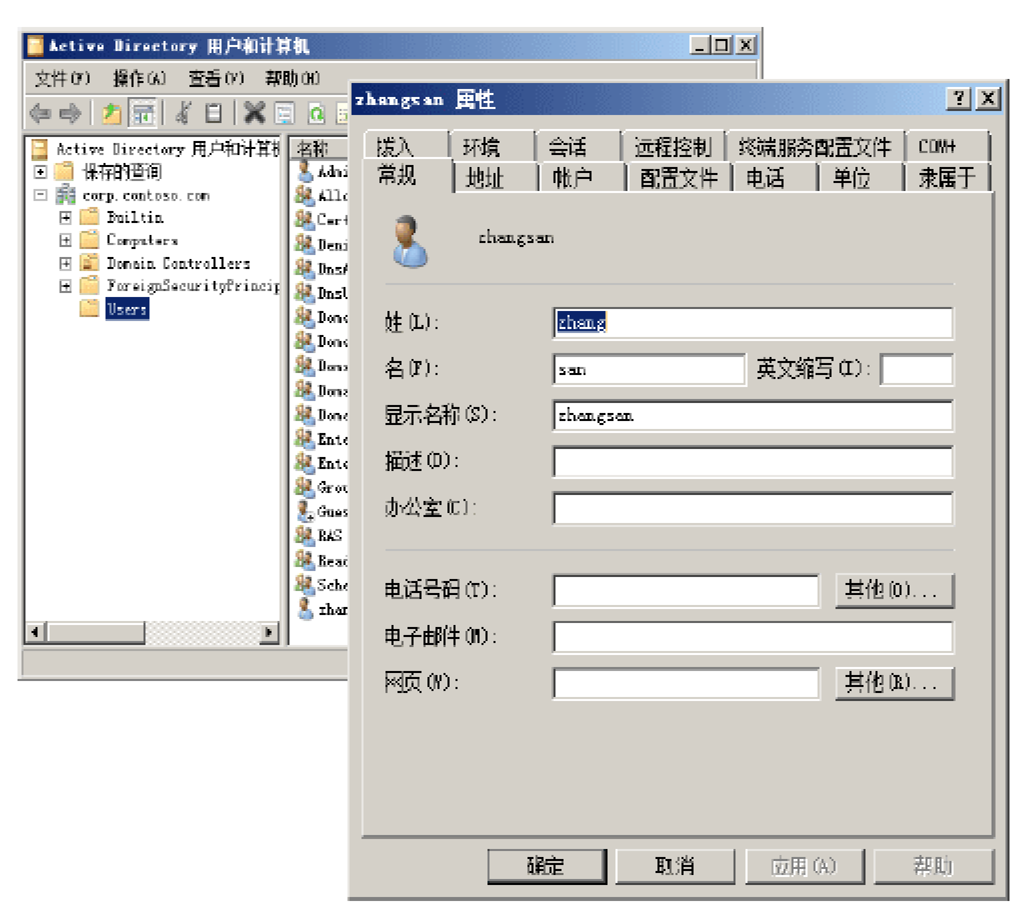
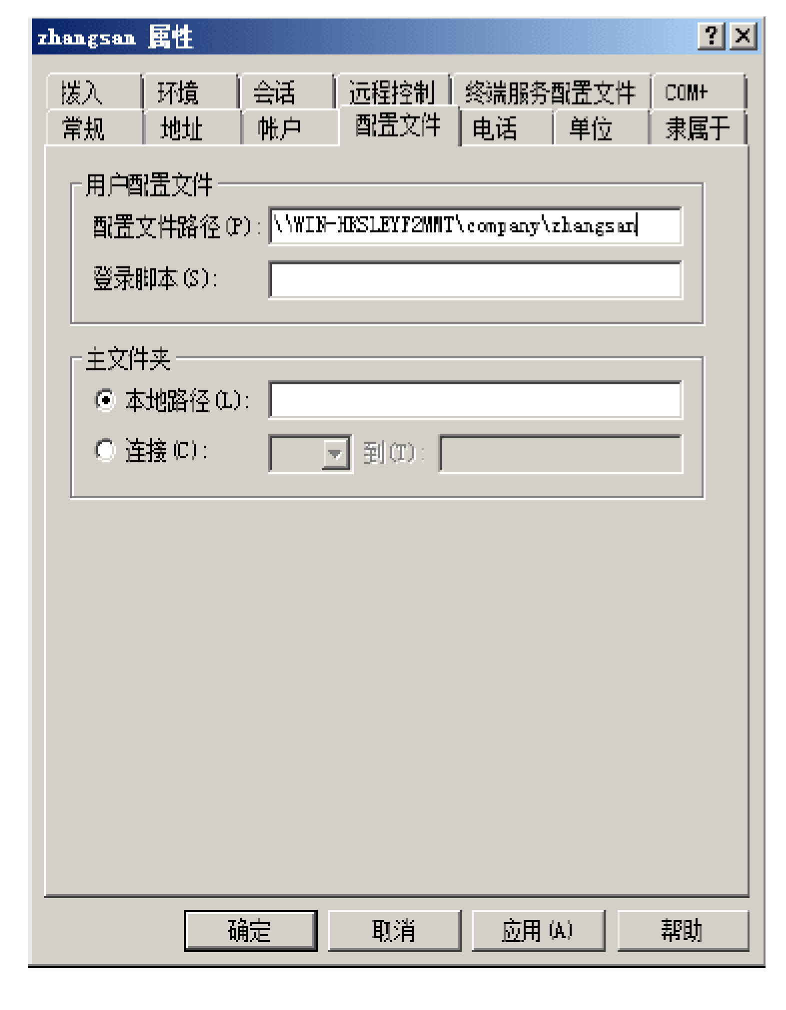


图 2.4 “zhangsan 属性”对话框

03 切换至“配置文件”选项卡，在“配置文件路径”文本框中输入存储 zhangsan 配置文件的 UNC 路径（网络路径）\\WIN-HKSLEYF2MMT\company\zhangsan（其中 WIN-HKSLEYF2MMT 为服务器名称，company 为存放该漫游用户配置文件的文件夹，zhangsan 为漫游用户配置文件的文件夹名称，该文件夹系统会自动创建）。完成后，单击“确定”按钮，显示如图 2.5 所示结果。

04 用 zhangsan 用户名登录可以看到服务器 company 文件夹下有一个 zhangsan 文件夹，显示如图 2.6 所示结果。





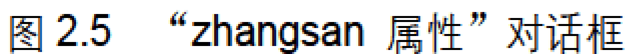


图 2.5　“zhangsan 属性”对话框

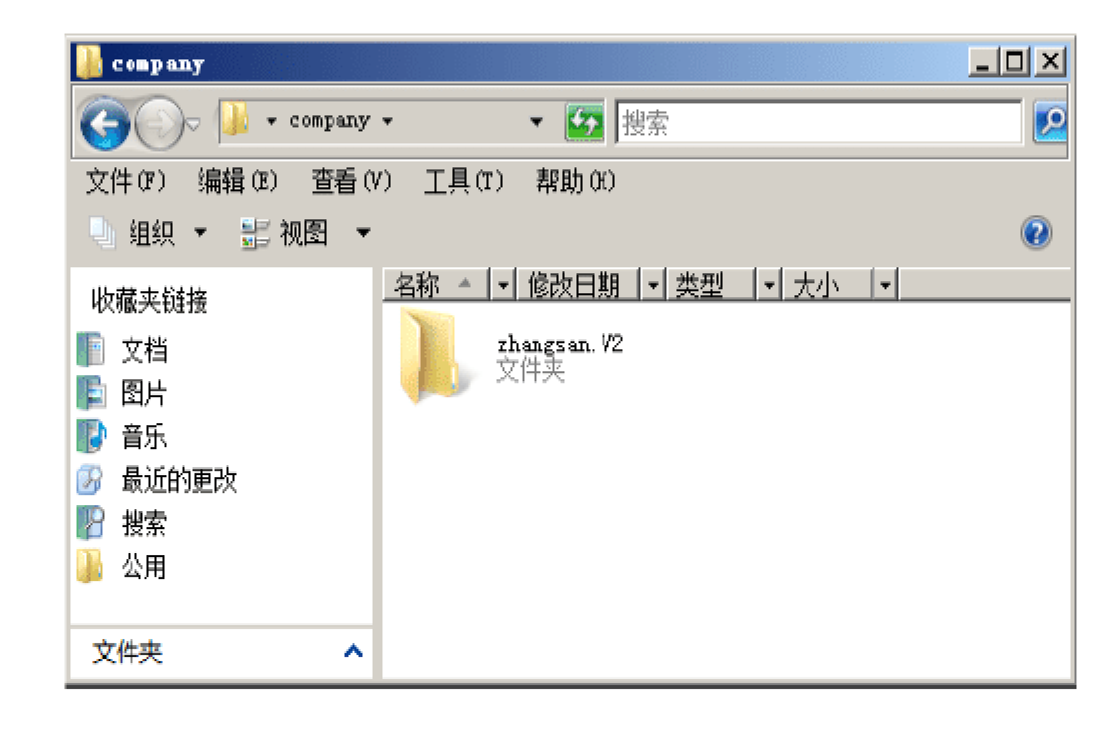
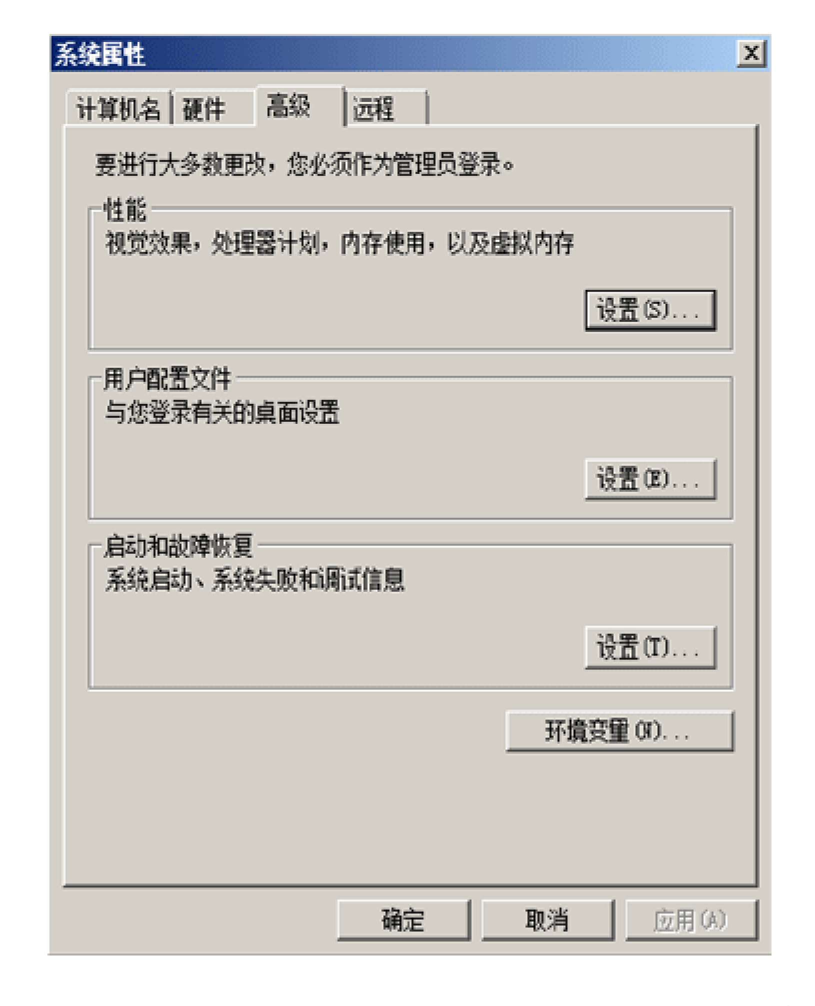


图 2.6　“zhangsan 的漫游用户配置文件夹”

（2）复制和指定漫游用户配置文件

管理员可以复制漫游用户配置文件并指定给其他用户使用。以 zhangsan 用户帐户为例，将其复制漫游配置文件复制到\\WIN-XPIJDUXAVLC\private\zhangsan 下。

01 以管理员身份登陆域控制器，选择“开始”→“控制面板”→“系统”→“高级系统设置”命令，显示“系统属性”对话框。切换至“高级”选项卡，“在用户配置”文本域中单击“设置”按钮，显示如图 2.7 所示 “用户配置文件”对话框。



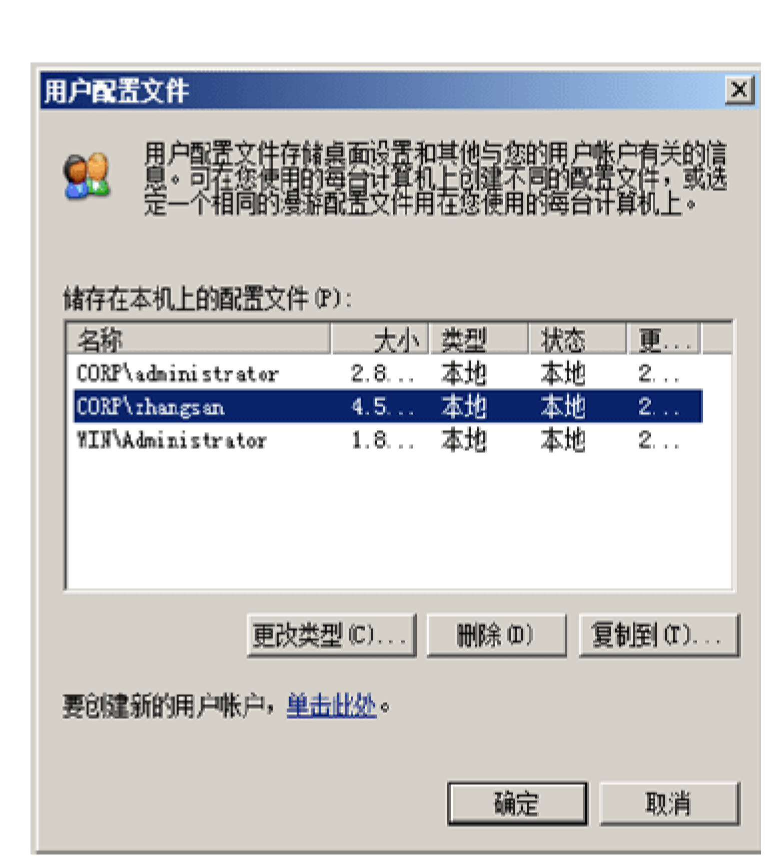


图 2.7　更改用户配置文件

02 选择用户 zhangsan，单击“复制到”按钮，出现如图 2.8 所示的“复制到”对话框，在“将配置文件复制到”文本框中输入目标 UNC 路径\\WIN-XPIJDUXAVLC\private\zhangsan。

03 单击“更改”按钮，显示如图 2.9 所示“Windows 安全”对话框，输入管理员帐户及密码。

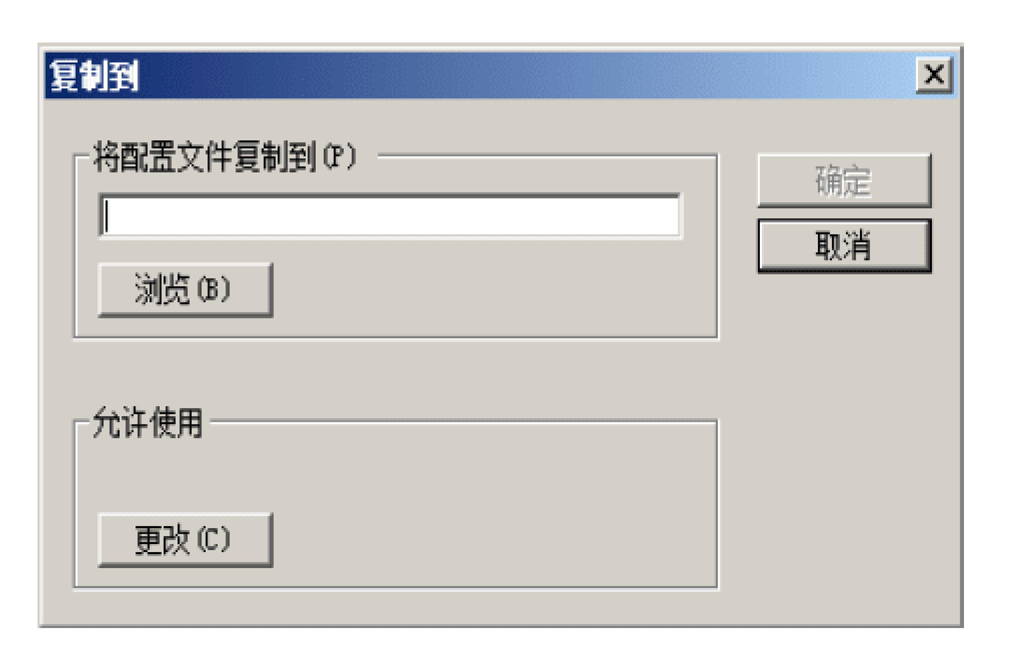


图 2.8 “复制到”对话框

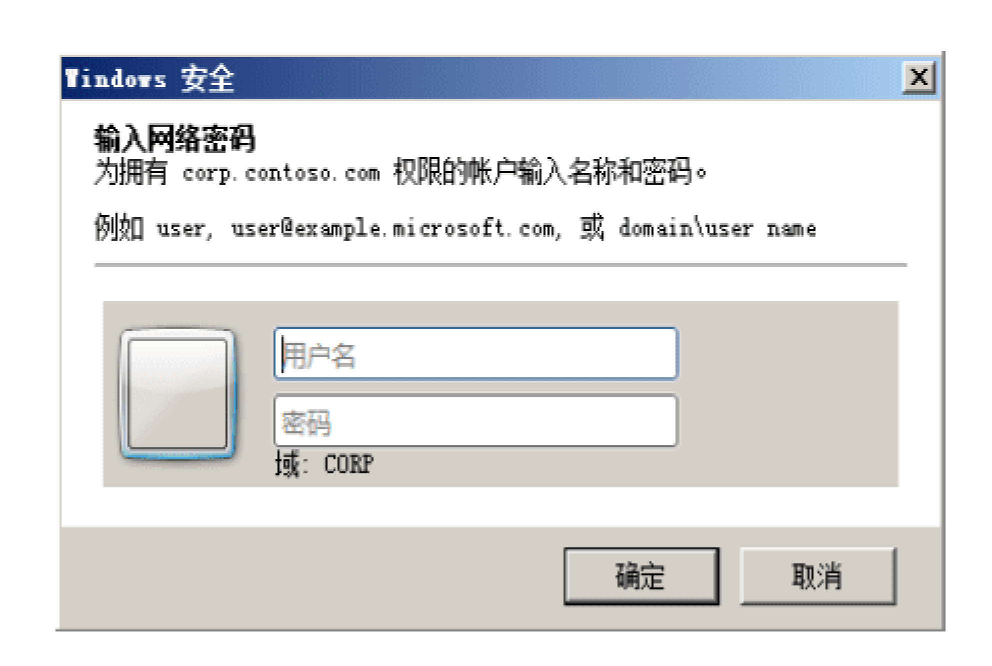


图 2.9 “Windows 安全”对话框

04 单击“确定”按钮，显示如图 2.10 所示“选择用户或组”对话框，在“输入要选择的对象名称”列表中，输入 zhangsan，或者单击“高级”按钮，以查找的方式选择该用户帐户。

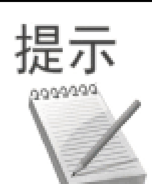
05 单击“确定”按钮，返回“复制到”对话框。继续单击“确定”按钮保存设置。



图 2.10 “选择用户或组”对话框

（3）强制用户配置文件

如果要固定用户的环境设置时，管理员可以使用强制用户配置文件，而该用户无法更改自己的用户配置文件。也就是说，当用户登录时可以更改当前的工作环境，但注销、重启后，这些更改不会被保存到域控制器上的强制用户配置文件内，再次登录时还是原来的固定环境。建立强制用户配置文件的方法与建立漫游用户配置文件的方法类似，只不过在漫游用户配置文件建立后，在服务器上的漫游用户配置文件夹内将 Ntuser.dat 文件改名为 Ntuer.man 即可。

提示  Ntuser.dat 文件是默认隐藏的，管理员可以在“工具”→“文件夹选项”→“查看”中取消“隐藏受保护的系统文件”和“显示隐藏的文件和文件夹”复选框。

2.1.2 登录脚本设置

所谓登录脚本，就是当用户登录计算机时自动执行的程序。登录脚本文件通常是批处理脚本文件、可执行文件或利用 VB 和 Jscript 编写的 Windows 脚本。管理员可以设计登录脚本来自动执行用户环境的配置过程。

1. 本地用户帐户登录脚本设置

如果要将登录脚本指派给本地用户可以进行如下操作：

01 以管理员帐户登录，创建登录脚本，选择“开始”→“运行”命令，打开“运行”对话框。在运行对话框中输入“gpedit.msc”命令，打开如图 2.11 所示“本地组策略编辑器”窗口。也可以直接在“开始搜索”文本框中输入“gpedit.msc”命令，回车执行打开该窗口。



02 依次选择“用户配置”→“Windows 设置”→“脚本”选项，在右侧窗口中双击“登录”选项，显示“登录 属性”对话框。单击“添加”按钮，显示如图 2.12 所示“添加脚本”对话框，在“脚本名”文本框中输入脚本路径。

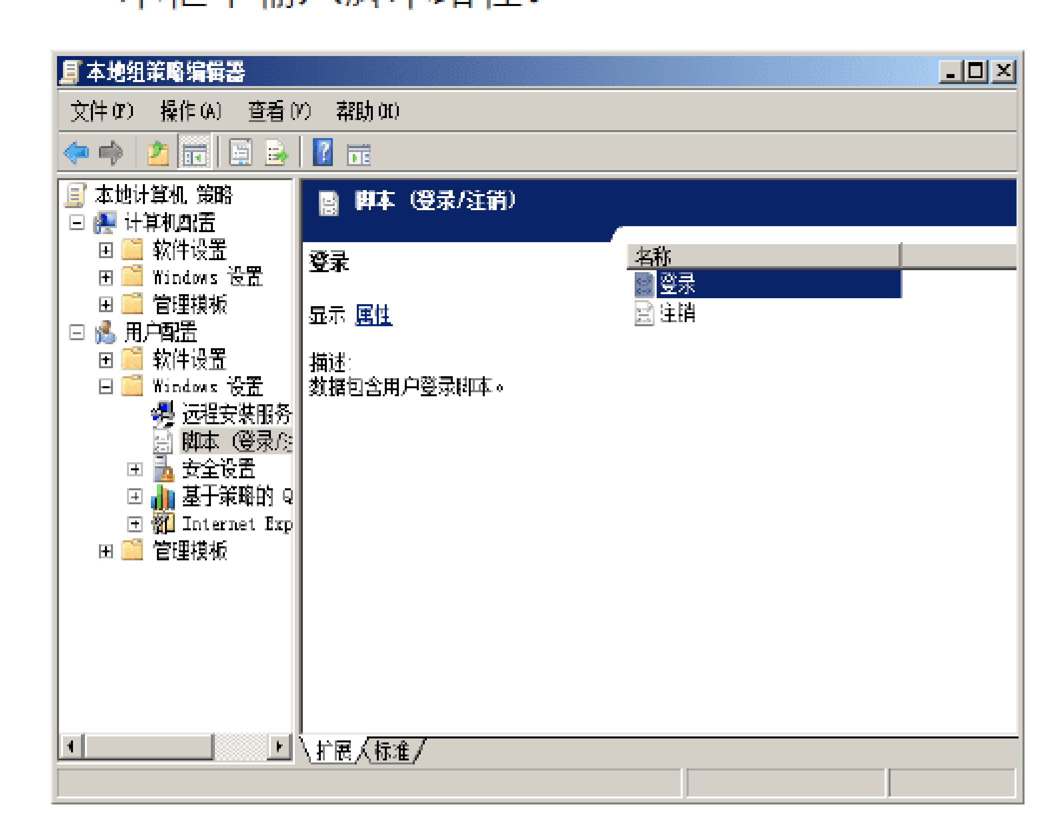


图 2.11　“本地组策略编辑器”对话框

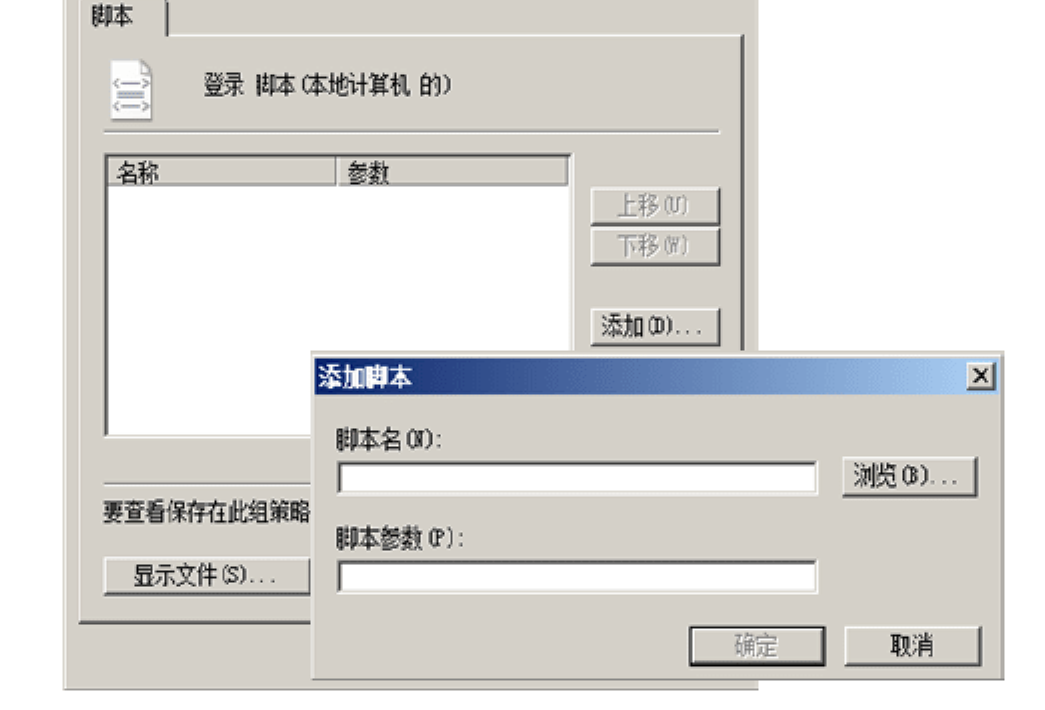


图 2.12　添加脚本

03 单击“确定”按钮，返回“登录 属性”对话框，单击“确定”按钮即可生效。

2. 域用户帐户登录脚本设置

如果要将登录脚本指派给域用户帐户（以 zhangsan 为例）可以进行如下操作。

01 创建登录脚本 nihao.vbs，然后将其复制到 C:\Windows\SYSVOL\domain\scripts 文件夹内。

02 选择“开始”→“管理工具”→“Active Directory 用户和计算机”命令，在 User 组中双击 zhangsan，显示“zhangsan 属性”对话框，切换至“配置文件”选项卡，在“登录脚本”文本框中输入登录脚本 nihao.vbs，如图 2.13 所示。

03 单击“确定”按钮保存设置即可。当 zhangsan 用户在网络上的任何一台计算机登录时，都会自动运行脚本 nihao.vbs，显示如图 2.14 所示“Windows Script Host”对话框。

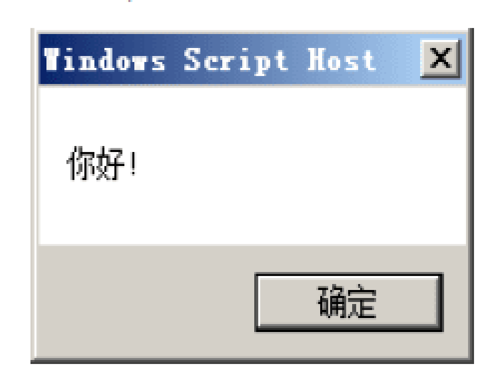


图 2.14　“Windows Script Host”对话框

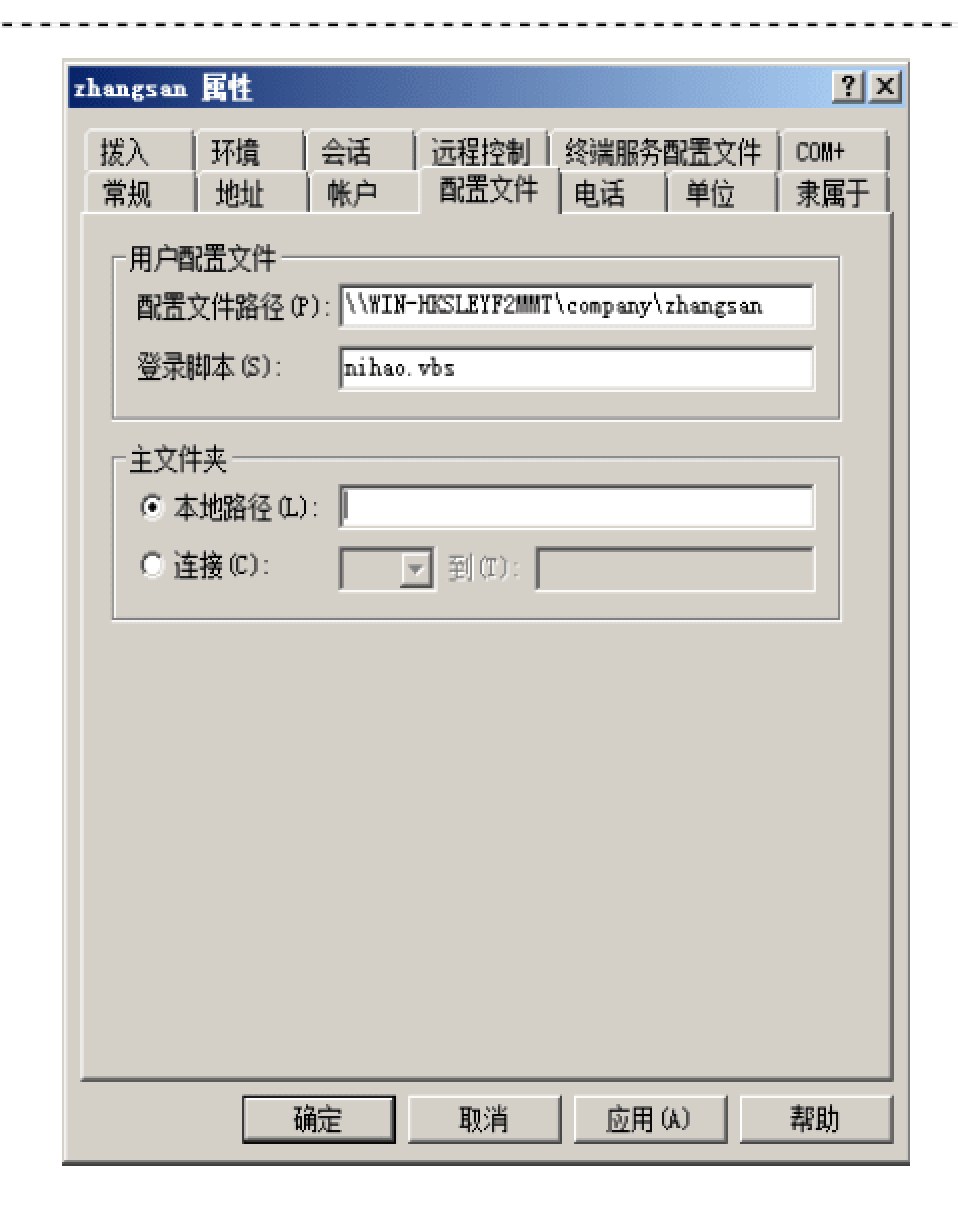


图 2.13　“zhangsan 属性”对话框

2.1.3　主文件夹设置

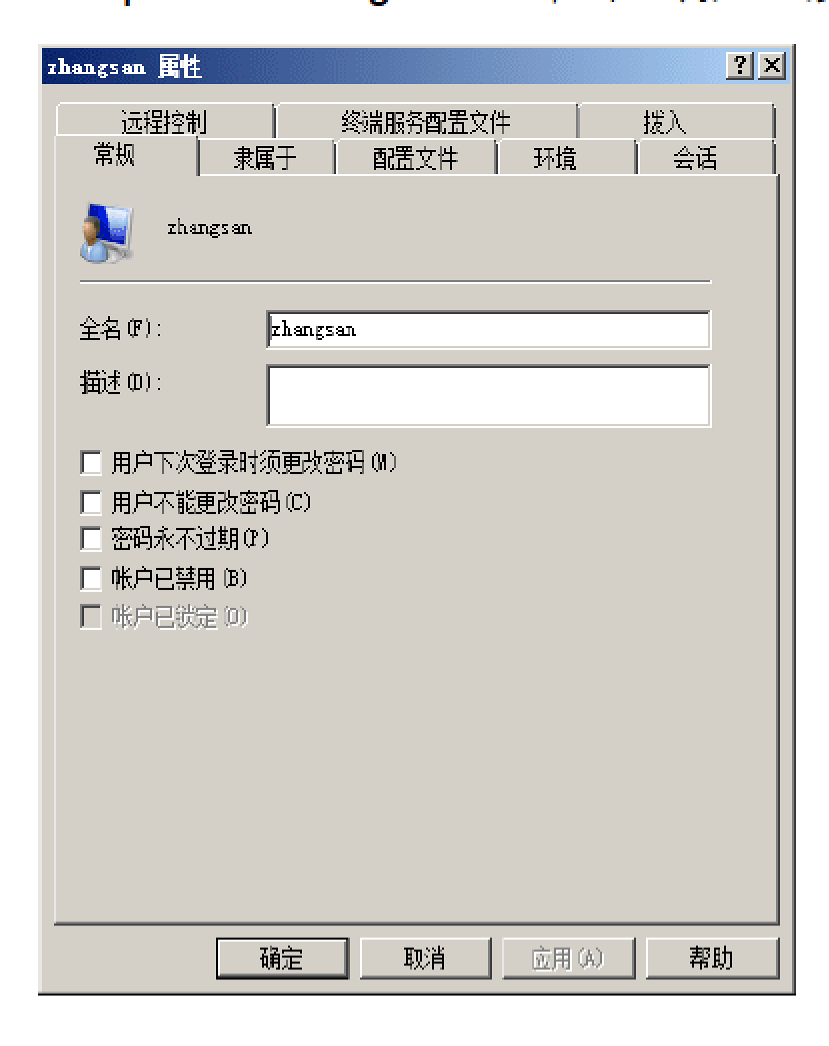
在 Windows Server 2008 中，每个域用户都有一个存储个人文件的位置，类似于我的文档，在

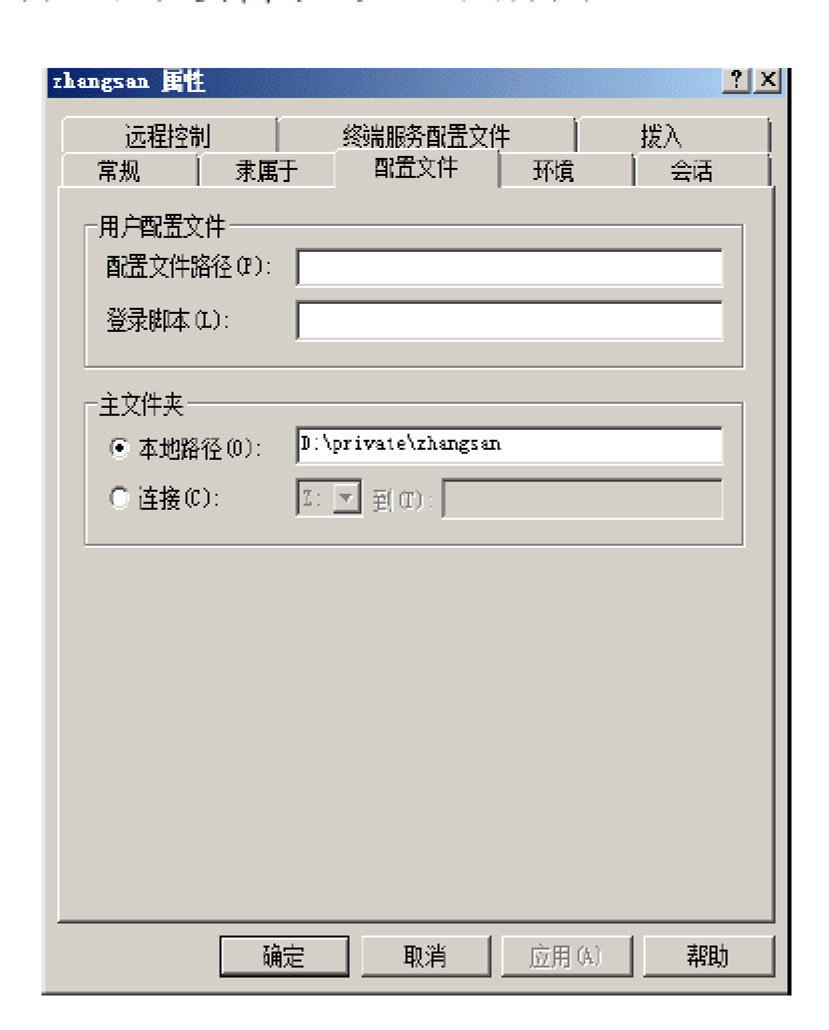
Windows Server 2008 中则是以用户名为该文档的文档名。该文档包含在用户配置文件内，所以域用户若使用漫游用户配置文件，则会在注销、登录时花费一定时间回存或下载该文档中的文件。除了用户文档外，Windows Server 2008 还提供了可以让用户存储个人文件的主文件夹。它只有所有者和 Administartor 才有权限访问主文件夹，并且该主文件夹不包含在用户配置文件内。

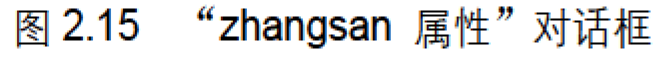
1. 本地用户主文件夹设置

01 以 Administrator 身份登录系统，选择“开始”→“管理工具”→“计算机管理”命令，打开“计算机管理”控制台。依次选择“本地用户和组”→“用户”选项，在“用户组中”选择用户（以 zhangsan 为例）并双击，显示如图 2.15 所示“zhangsan 属性”对话框。

02 切换至“配置文件”选项卡，在本地路径文本框中输入主文件夹的相对路径，显示如图 2.16 所示结果，例如：“D:\private\zhangsan”，单击“确定”按钮后，系统会自动创建主文件夹。






图 2.15 “zhangsan 属性”对话框　　图 2.16 “配置文件”选项卡

注意 

如果主文件夹位于 NTFS 分区上，则系统会自动将该文件夹的权限设置给用户。不要将主文件夹建立在网络上的共享文件夹内，因为系统不会建立该文件夹，也无法设置其权限，在网络连接失败时，主文件夹也就不存在了。

---

2. 域用户帐户主文件夹设置

01 以 Administrator 身份登录系统，依次选择“开始”→“管理工具”→“Active Directory 用户和计算机”选项，打开“Active Directory 用户和计算机”窗口。

02 在相应的组织单位中选择用户（以 zhangsan 为例），双击“zhangsan”用户，显示“zhangsan 属性”对话框。切换至“配置文件”选项卡，如果要设置在本地计算机内，则在“本地路径”文本框中输入本地相对路径，如果设置在网络上的某台计算机的共享文件夹内，则单击“连接”单选按钮，在盘符下拉列表中选择主文件夹的驱动器位置，在“连接”文本框中输入 UNC 路径如\\WIN-HKSLEYF2MMT\2008\zhangsan，显示如图 2.17 所示结果。



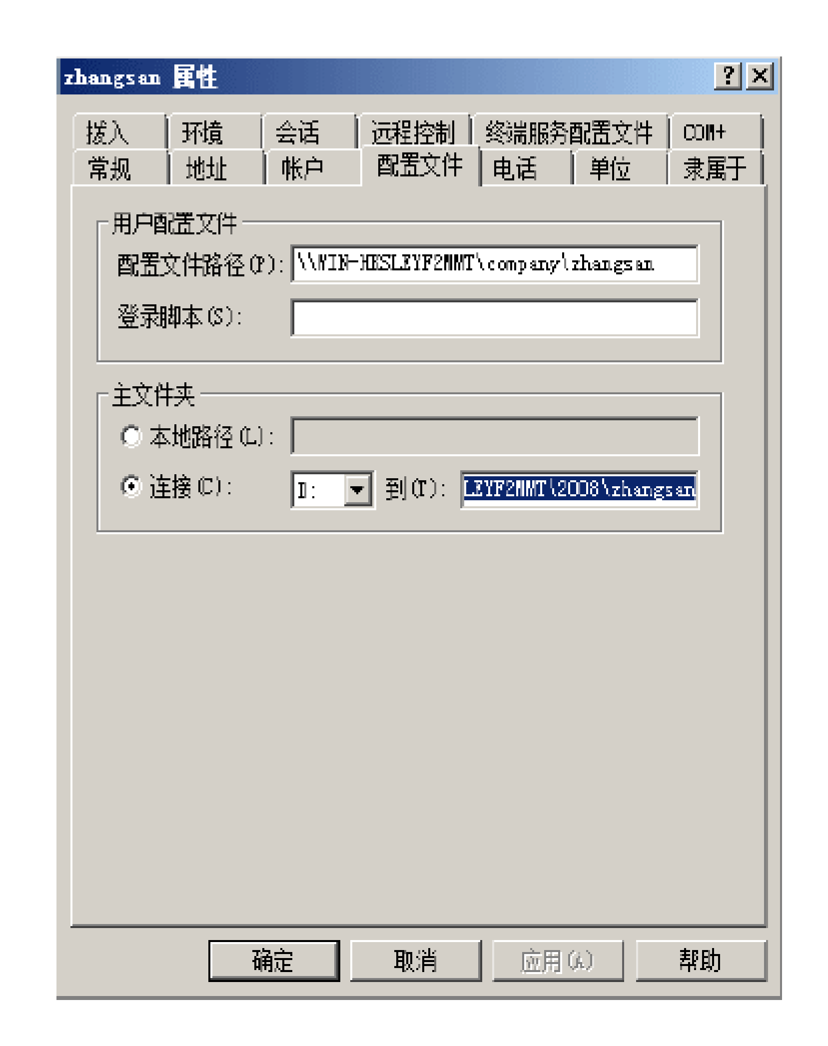


图 2.17　“zhangsan 属性”对话框

03 单击“确定”按钮保存设置。

2.1.4　重定向用户配置文件设置

Windows Server 2008 系统中，所有用户帐户的配置文件都被保存在系统分区中，包括收藏夹、保存的游戏、连接、视频、联系人。如果没有备份，那么当系统崩溃或重新安装系统时，这些私人信息将全部丢失。最好的方法是，将这些重要的内容重定向到其他安全的非系统磁盘上。

1. 重定向 zhangsan 的下载文件夹

01 依次打开“计算机”→“本地磁盘（C:）”→“用户”→“zhangsan”文件夹，右击下载文件夹选择“属性”命令，打开文件夹属性对话框，切换至“位置”选项卡，单击“移动”按钮，显示如图 2.18 所示“选择一个目标”窗口，选择一个安全磁盘或文件夹即可。

02 单击“选择文件夹”按钮，返回“桌面 属性”对话框，单击“确定”按钮，显示如图 2.19 所示“移动文件夹”对话框，单击“确定”按钮即可完成。

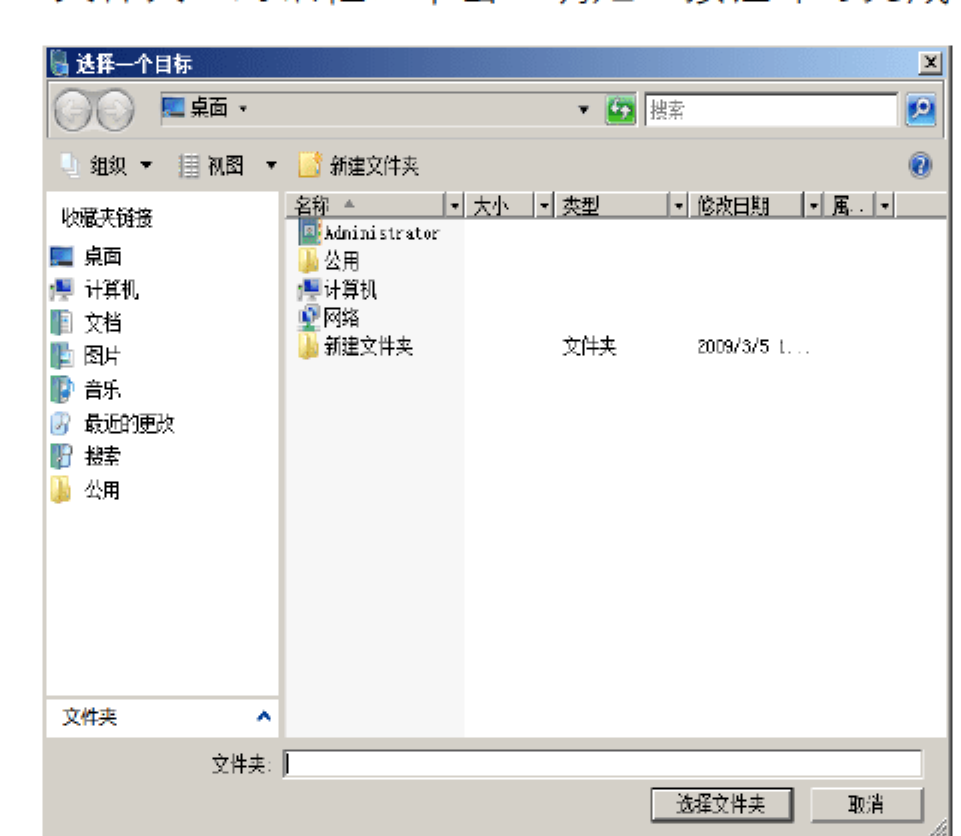


图 2.18　“选择一个目标”对话框

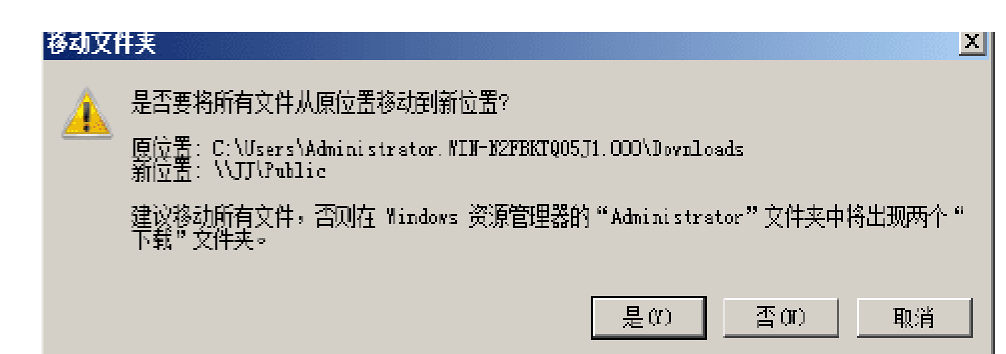


图 2.19　“移动文件夹确定”窗口



提示

用户帐户只能重定向自己的配置文件，管理员也无法重定向其他用户配置文件。

2. 重定向程序安装目录“Program Files”

所有用户默认安装的应用程序都装在 C:\Program Files，随着应用程序的不断增加，此文件夹不仅会占用大量的空间，也不利于应用程序的安全。通过修改注册表将默认安装目录重定向到其他磁盘即可。

01 打开“注册表编辑器”窗口，依次展开 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion 分支。在右侧列表中双击“ProgramFilesDir”键值，显示如图 2.20 所示“编辑字符串”对话框。在“数值数据”文本框中输入更改后的路径。

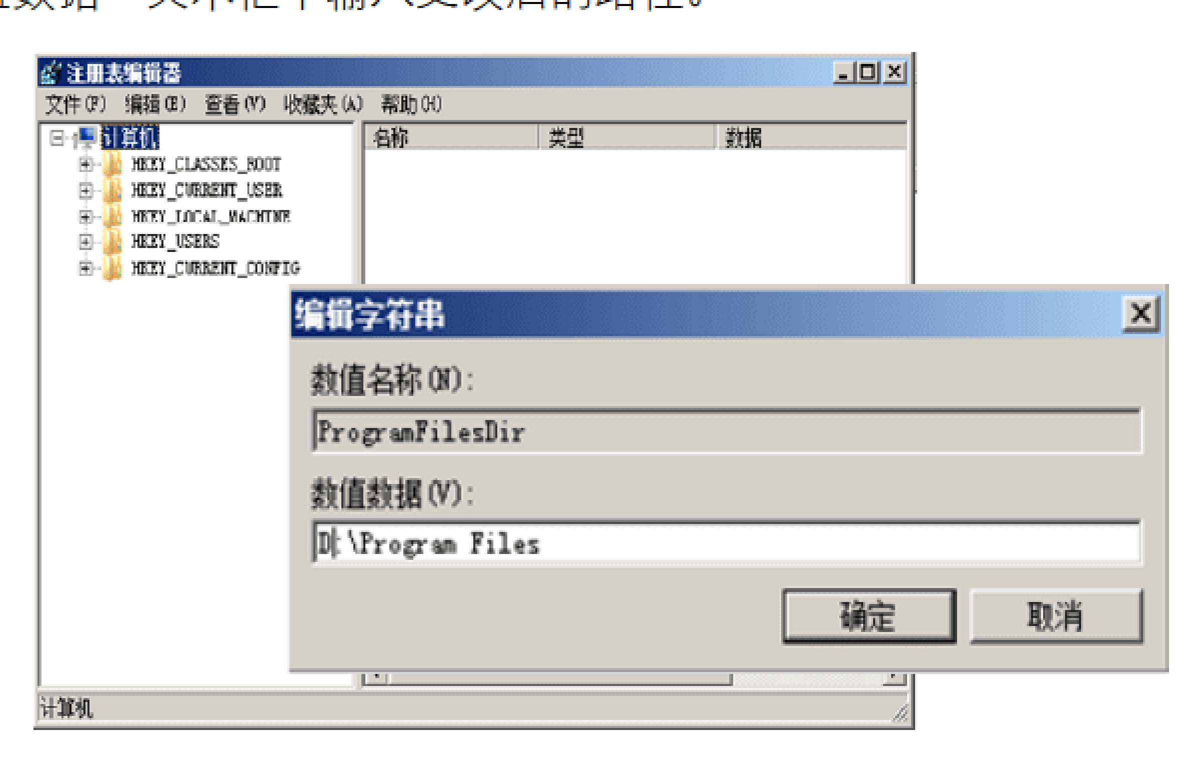


图 2.20 编辑字符串

02 单击“完成”按钮，重启系统后所做修改即可生效。

3. 重定向“IE 临时文件夹”

服务器虽不经常上网，但偶尔也会由于业务需要访问 Internet，使用 IE 浏览器浏览网页时，会产生一些临时文件，随着时间的积累，这些临时文件就会非常庞大，不仅占用宝贵的系统分区空间，而且容易留下安全隐患。通过将保存临时文件的文件夹重定向到其他分区，即可解决该问题。

01 打开 IE 浏览器，在菜单栏中选择“工具”，在菜单列表中选择“Internet 选项”，显示如图 2.21 所示“Internet 选项”对话框。

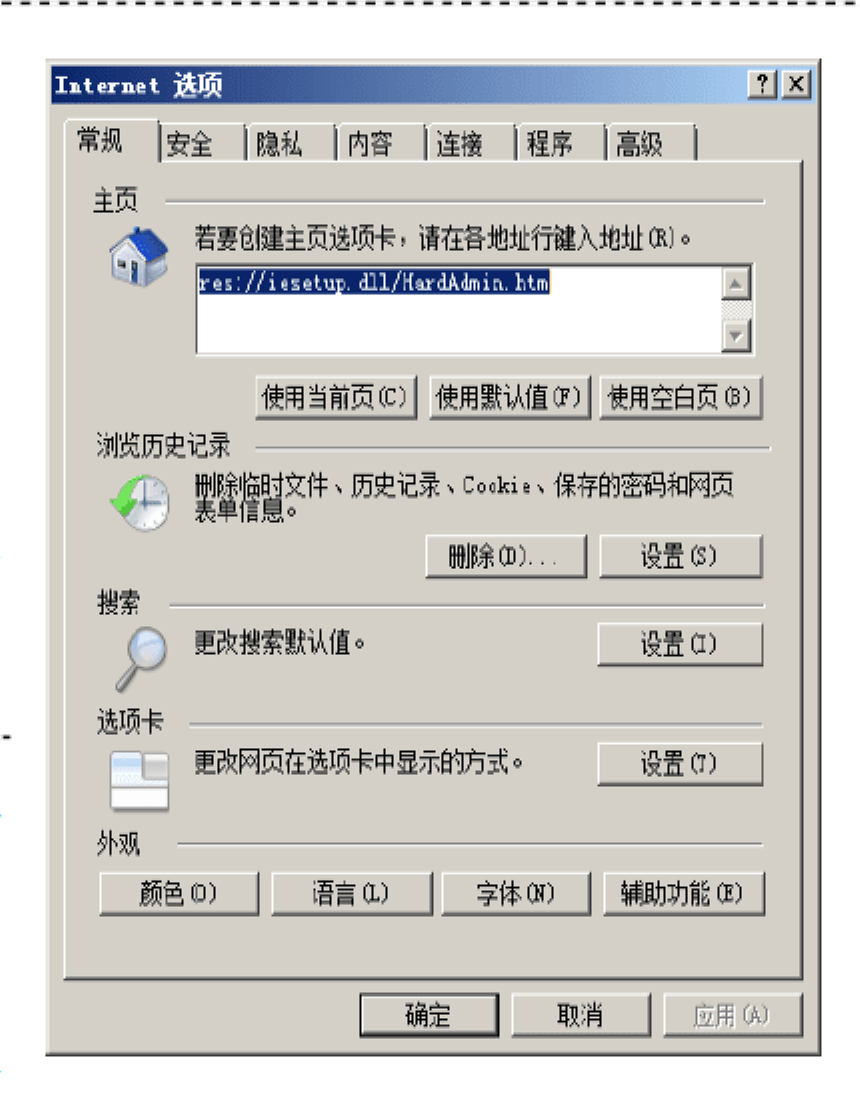


图 2.21 “Internet 选项”对话框

02 单击“常规”选项卡，在“Internet 临时文件”区域中，单击“设置”按钮，显示“设置”对话框。系统默认的临时文件夹的位置为“C:\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files”，单击“Internet 临时文件夹”区域中的“移动文件夹”按钮，显示“浏览文件夹”对话框，选择文件夹的目标位置即可，如图 2.22 所示。



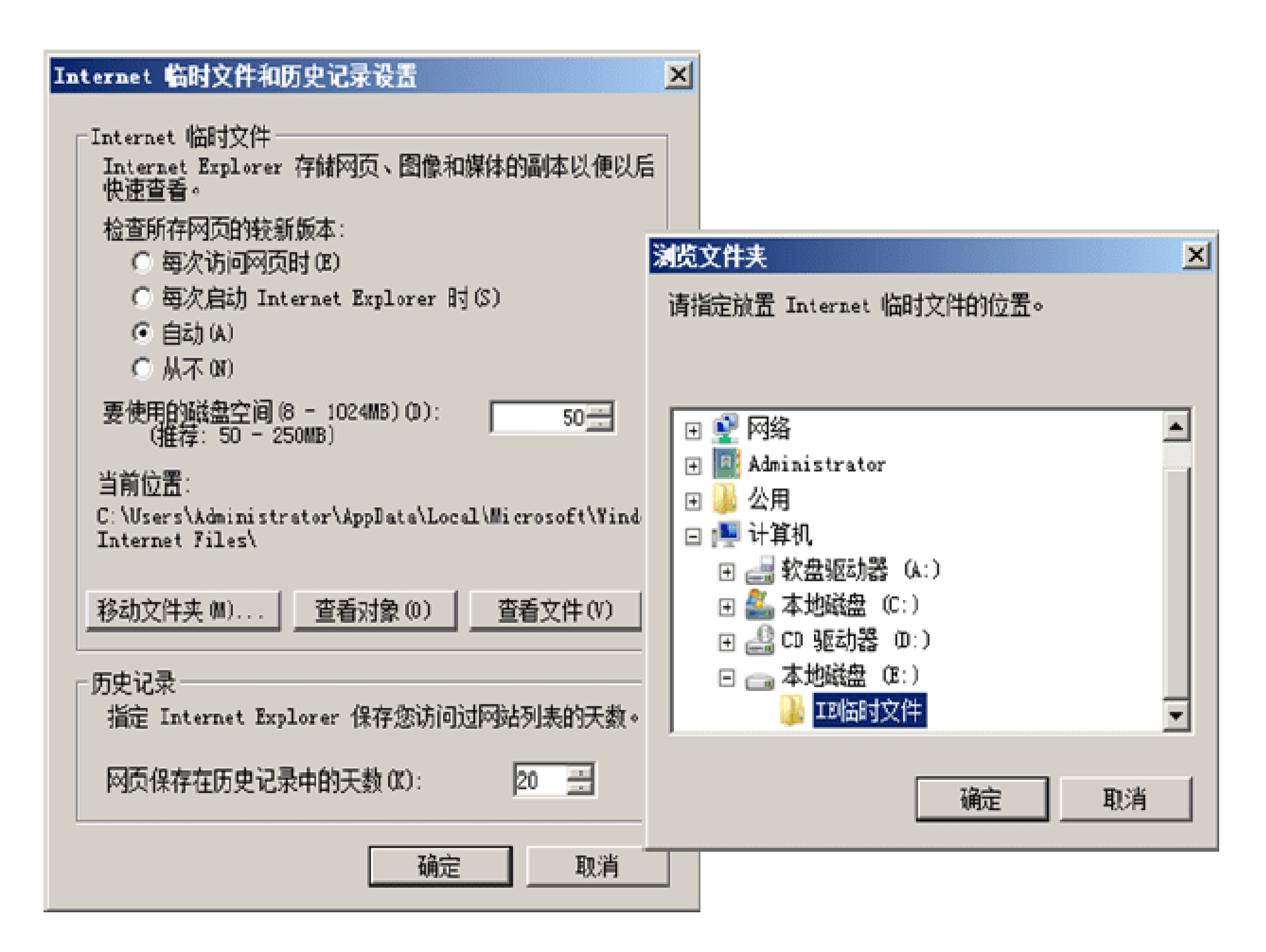


图 2.22　设置 Internet 临时文件夹

03 依次单击“确定”按钮，保存设置。此时会提示如图 2.23 所示“注销”对话框。单击“是”按钮，系统自动执行注销操作。重新启动后，“IE 临时文件夹”生效。



图 2.23　“注销”对话框

2.2　Internet Explorer 浏览器安全设置

Windows Internet Explorer 是微软公司推出的一款网页浏览器，通过 Internet Explorer 可以轻松获取丰富的 Internet 信息。Internet Explorer 7（简称 IE 7）是目前最安全的 Internet Explorer 版本，支持翻页浏览、RSS 订阅、页面缩放、快速切换等功能，以及具有 Anti-Phishing 过滤器（反网络钓鱼）和仿冒网站筛选等动态安全，在一定程度上增强了 Internet Explorer 的安全性。

2.2.1　安全配置功能

IE 7 在 IE 6 的基础上新增了多项安全功能设置，主要安全配置功能如下。

1. 防范钓鱼欺诈网站

IE 7 推出了网钓过滤器，避免用户在仿冒的钓鱼欺诈页面输入个人的帐户或密码遭有心人士的收集和身份被冒用。网钓过滤器会自动检查用户所访问的网站，并与一致的网钓黑名单进

行对比分析。如果该站被识别出为钓鱼欺诈网站或与钓鱼欺诈网站相符，那么过滤器就会显示警告窗口，提示用户该网站被报告为钓鱼欺诈网站，并建议用户关闭该网页。

2. ActiveX 的选择加入功能

用户可以逐一解除每个网页内容“区域”的 ActiveX 选择加入功能。针对“Internet”和“限制的网站”而言，这项“选择加入”功能缺省为开启的，以提升安全性，但对“近端内部网络”（Intranet）与“信任的网站”而言，缺省为关闭的。

3. 跨域安全

IE 7 的新安全机制会阻止一种叫“跨域脚本（cross-domain scripting）”的攻击策略。为了防止恶意代码利用合法网站中的薄弱代码漏洞，IE 7 会迫使脚本仅运行其初始的安全内容，哪怕它已被重定向到一个完全不同的安全域上。

4. 锁定安全区域

由于安全环境缺省在更高层级，IE 7 的安全区域锁得比以往更加严密，包括取消非域名电脑上的近端内部网络区域，并且新的界面让人更难选择低级或中低级的安全性。

5. 更强的 SSL/TLS 通知与数字认证信息

IE7 的使用者可轻易地判断某个网站释放具有 SSL/TLS 安全性，并取得该完整的数字认证信息。若网站具有高可靠度认证，浏览器网址列的颜色会变绿。

6. 隐私保护功能

通过修改注册表中的相关键值，即可阻止 HTML 获取用户个人信息，即用户可以很容易地清除在网页中已经输入过的用户帐户和密码、临时文件、历史记录、Cookies 及其他个人信息。

7. 固定地址栏

IE7 中所有浏览器窗口均提供地址栏，所以恶意网站难以再通过隐藏该网站的 URL 地址达到隐满用户的目的。

8. 国际字符警告

IE7 支持国际字符集，为了防止不法分子利用不同语言字符的相似性进行欺骗，每当用户使用国际字符集时，如果出现属于另一种语言的字符，浏览器会提醒用户注意。

2.2.2 开启仿冒网站筛选

仿冒网站筛选是 Internet Explorer 中一种帮助检测仿冒网站的功能。仿冒网站筛选功能的实现过程如下：

- 首先，将访问的网站地址与向 Microsoft 报告为合法站点的站点列表进行比较。该列表保存在您的计算机上；



■ 其次，帮助分析访问的站点，以查看它们是否具有仿冒网站中常见的特征；

■ 最后，在用户同意的前提下，将一些网站地址发送给 Microsoft，以便根据频繁更新的已报告仿冒网站列表进行进一步的检查。

01 打开 IE 浏览器，选择“工具”→“Internet 选项”命令，显示如图 2.24 所示的“Internet 选项”对话框。

02 切换至“高级”选项卡，显示如图 2.25 所示的“高级”选项卡，在“安全”区域中找到“仿冒网站筛选器”，选中“打开自动网站检查”单选按钮。

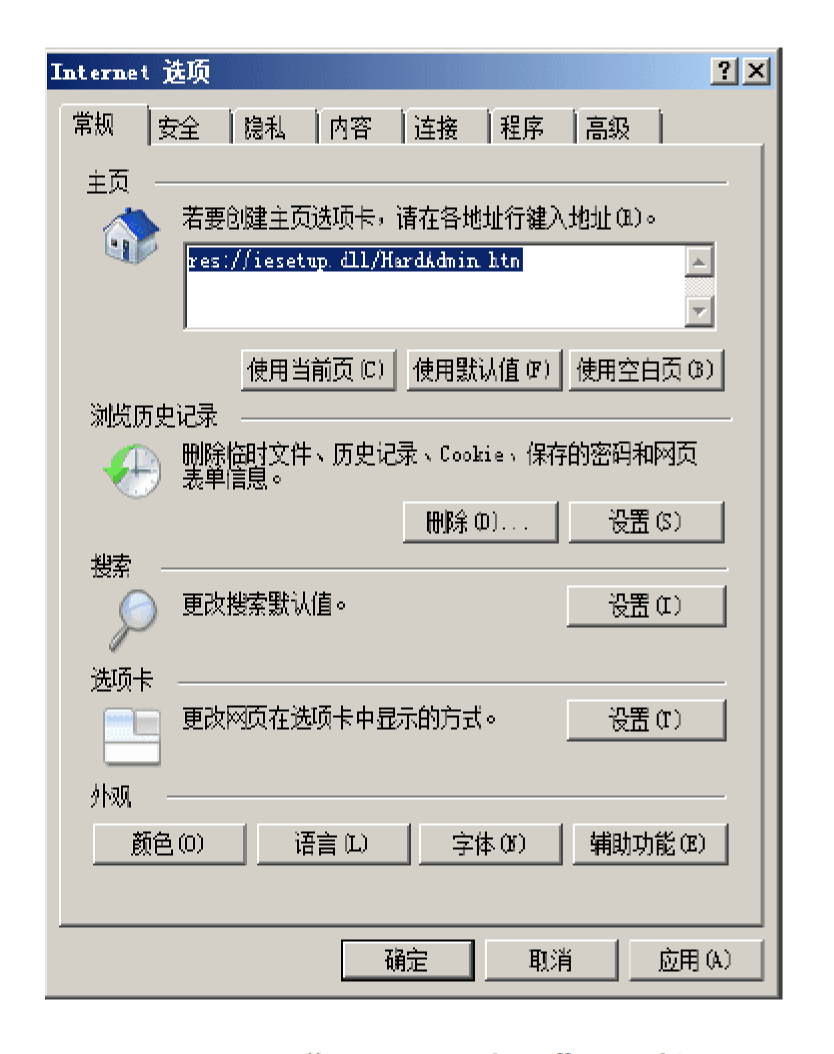


图 2.24　“Internet 选项”对话框

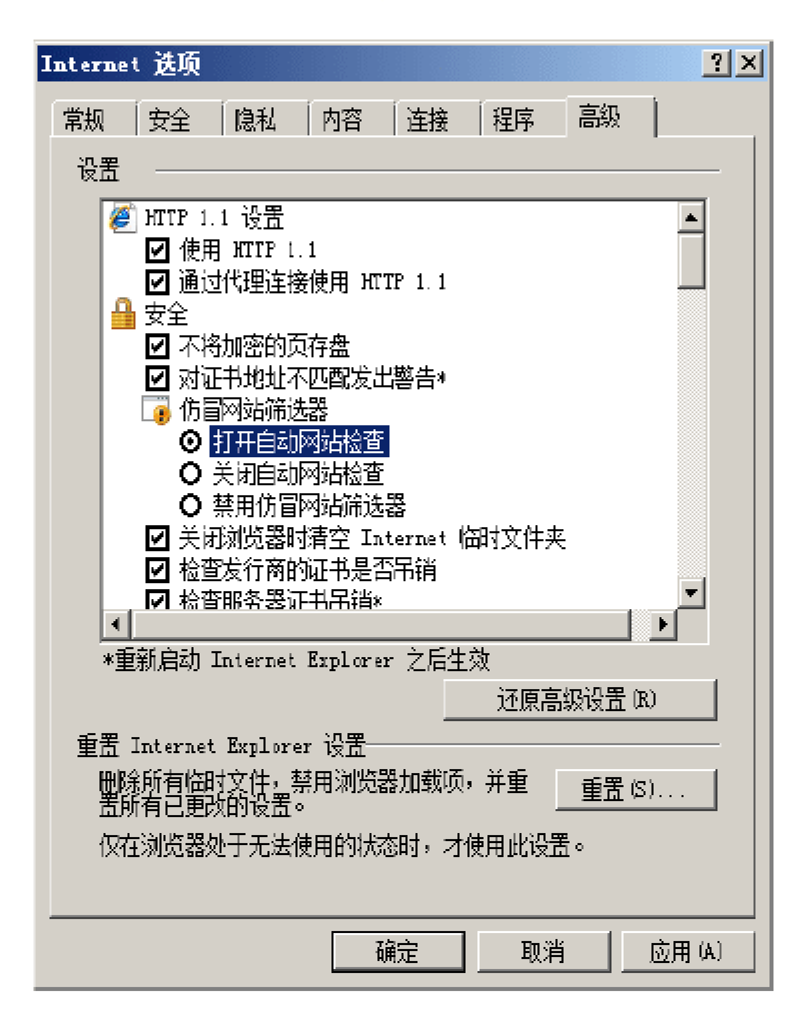


图 2.25　“高级”选项卡

03 单击“确定”按钮，显示如图 2.26 所示“仿冒网站筛选”对话框，单击“确定”按钮即可。

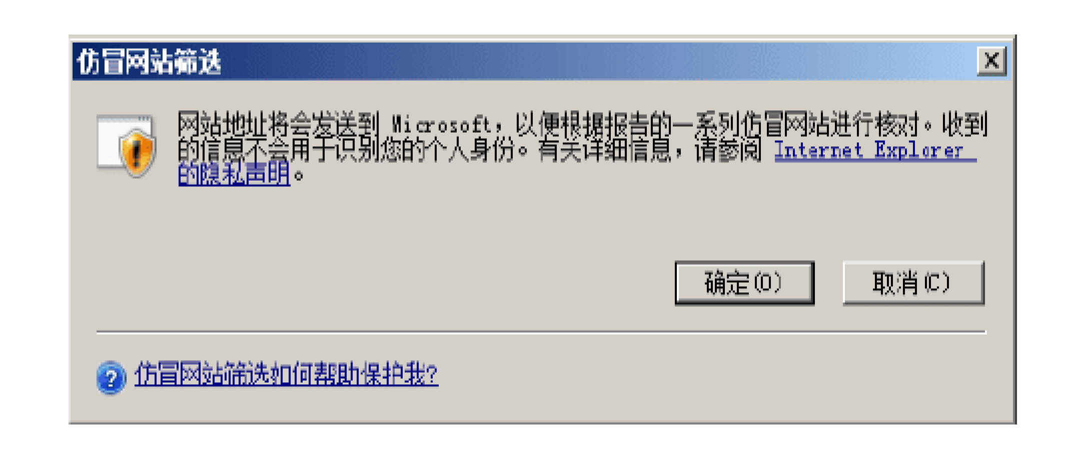


图 2.26　“仿冒网站筛选”对话框

2.2.3　管理加载项

有些与 IE 浏览器配合使用的应用程序，往往会自动嵌入到 IE 7 中，每次打开浏览器，都会自动运行该程序，如搜索工具、域名转换工具等。管理员可以通过禁止其对应的加载项，从而避免其随 IE 7 自动运行。

01 在 IE 7 菜单栏中选择“工具”→“加载选项”→“启用或禁用加载项”命令，显示如图 2.27 所示“管理加载项”对话框。

02 在“显示”下拉列表中选择“Internet Explorer 当前加载的加载项”，在下面文本框中显示了已经使用的加载项。选中不必要加载的加载项，在设置选项区域选中“禁用”单按钮，显示如图 2.28 所示“管理加载项”提示框。



图 2.27 “管理加载项”对话框



图 2.28 “管理加载项”提示框

03 单击“确定”按钮，重新启动 IE 浏览器即可生效。

小　　结

Windows Server 2008 提供了一些新的和改进的安全技术，增强了对系统的保护，为企业提供了一个安全平台。本章主要讲了 Windows Server 2008 系统下的用户环境安全设置，包括工作环境设置和 IE7 安全设置。用户所有的工作环境信息都是被保存在用户配置文件中的，而用户配置文件根据用途和功能不同又可以分为 4 种类型，分别是本地用户配置文件、漫游用户配置文件、强制用户配置文件和临时用户配置文件。IE 浏览器在服务器上虽不常用，但却是许多安全漏洞的藏身支持，为此，管理员应从多方面加强 IE 浏览器的安全设置。

习　　题

1. 在 Windows Server 2008 中，用户工作环境有哪些内容？
2. IE 7 具有哪些新增安全功能？
3. 如何对 IE 7 进行安全设置？



实验：配置用户工作环境

实验目的

在 Windows Server 2008 中，掌握系统用户工作环境的配置方法。

实验内容

Windows Server 2008 安装完成后，对用户工作环境设置，包括用户桌面的设置、应用程序的设置、文件夹设置、磁盘配额设置等。

实验步骤

1. 设置本地用户配置文件和漫游用户配置文件。
2. 分别将登录脚本指派给本地用户和域用户帐户。
3. 对本地用户和域用户帐户设置主文件夹。
4. 重定向用户配置文件设置。
5. 为用户设置适合的磁盘配额。

Windows Server 2008

第3章

修补系统漏洞

系统漏洞是指应用软件或操作系统软件，在逻辑设计上的缺陷或在编写时产生的错误，而这些缺陷或错误有可能被非法用户利用，并将木马或病毒等有害程序安装到本地计算机或者远程控制计算机，从而窃取重要资料和信息，甚至破坏系统。Windows Server 2008 相对于其他版本的 Windows 操作系统而言，安全性已经有了很大提高，但几乎每天都会有新的漏洞被发现。目前，及时安装系统更新是应对系统漏洞最有效的方法。

本章导读

- 什么是系统漏洞
- 扫描隐藏的漏洞
- 漏洞扫描工具 MBSA
- 其他常用扫描漏洞工具
- 修补系统漏洞的原则
- 微软免费修补漏洞工具



3.1　什么是系统漏洞

客观地讲，系统漏洞是无法避免的，对于 Windows 操作系统而言，新版的操作系统在弥补旧版的操作系统漏洞同时，还会引入一些新的漏洞。应对系统漏洞最有效的方法就是制定完善的修补策略，及时修补漏洞。漏洞除了系统（硬件、软件）本身固有的缺陷之外，还包括用户的不正当配置、管理以及制度上的风险，或其他非技术性因素造成的系统不安全。

3.1.1　漏洞的特性

通常情况下，普通用户都是在产品供应商公布产品漏洞后，才得知漏洞消息的。从信息安全的角度看，是先有漏洞和对漏洞攻击的可能性，后有补丁出现。漏洞是攻击者所要攻击的目标，而安装补丁是对漏洞的修补过程。漏洞是广泛存在的，不同的设备、操作系统以及应用系统都会存在安全漏洞。

1. 漏洞的时间局限性

任何系统漏洞都是用户在不断地使用过程中被发现，随之系统供应商采取新版本替代旧版本，或是发布补丁程序等方式弥补漏洞。随着旧漏洞的消失，新环境下的新漏洞也将随之产生。因此，系统漏洞只是存在于特定时间和环境下的，即只能针对目标系统的系统版本、其上运行的软件版本，以及服务运行设置等实际环境。

2. 漏洞的广泛性

漏洞会影响到大范围的软、硬件设备，包括操作系统本身及其支撑软件平台、网络客户端和服务器软件、网络路由器和安全防火墙等。换言之，在这些不同的软硬件设备中，可能都存在不同的系统漏洞问题。例如，不同种类的软、硬件设备之间，同种设备的不同版本之间，以及不同设备构成的不同系统之间，同种系统在不同的设置条件下，都会存在不同的安全漏洞。

3. 漏洞的隐蔽性

安全漏洞是最常见的系统漏洞类型之一。入侵者借助这些漏洞，可以绕过系统中的许多安全配置，从而实现入侵系统的目的。安全漏洞的出现，是由于对安全协议的具体实现中发生了错误，意外出现的非正常情况。而在实际的系统中，都会存在不同程度的潜在错误。因而所有系统中都存在安全漏洞，无论这些漏洞是否已被发现，也无论该系统的安全级别如何。在一定程度上，安全漏洞问题是存在于系统本身的理论安全级别上的。也就是说，并不是系统所属的安全级别越高，系统中所存在的漏洞就越少。

4. 漏洞的被发现性

漏洞是特定环境和时间内的必然产物，只有发现后，才会被用来入侵系统或被弥补。在实

际使用中，用户会发现系统中存在错误。入侵者会利用其中的某些错误，使其成为威胁系统安全的工具，也就是常说的系统安全漏洞。系统供应商发现后会尽快发布针对这个漏洞的补丁程序，纠正这个错误。这就是系统安全漏洞从被发现到被纠正的一般过程。

3.1.2 漏洞生命周期

漏洞所造成的安全问题具备一定的时效性，也就是说每一个漏洞都存在一个和产品类似的生命周期的概念。只有对漏洞生命周期的概念进行研究并且分析出一定的规律，才能达到真正解决漏洞危害的目的。

漏洞生命周期的定义：漏洞从客观存在到被发现、利用，到大规模危害和逐渐消失，这期间存在一个生命周期，该周期被称为漏洞生命周期。

以“冲击波（MSBlaster)”蠕虫病毒为例，漏洞生命周期的包括如下 5 个基本阶段。

第 1 阶段：发现漏洞

2003 年 7 月 16 日，微软公司公布了 MS03-026 Microsoft Windows DCOM RPC 接口远程缓冲区溢出漏洞，该漏洞影响 Windows 2000、Windows XP、Windows Server 2003 系统。

第 2 阶段：弥补漏洞

2003 年 7 月 16 日，微软公司公布了 MS03-026 补丁用于修补该漏洞。随后，在微软发布该漏洞后，网络上有零星的恶意攻击者利用该漏洞进行入侵。

第 3 阶段：利用漏洞的病毒大肆爆发

2003 年 8 月 11 日，爆发了利用上述 Windows 漏洞的“冲击波”蠕虫病毒。

第 4 阶段：病毒出现变种

2003 年 8 月 18 日，出现了一个利用同样原理进行蔓延的“冲击波清除者”病毒，该蠕虫专门清除原来的冲击波病毒，然而这个病毒却消耗了大量的 Internet 带宽，导致 Internet 性能显著下降。

从蠕虫爆发后全球 Windows 用户开始安装 MS03–026 补丁修补该漏洞，网络运营商开始设法阻止蠕虫蔓延，计算机防病毒厂商加入蠕虫特征进行查杀。

第 5 阶段：逐渐消失

2004 年 1 月，蠕虫传播开始明显被遏制，微软公司估计全球有 1000 万台主机受到感染。从整个事件开始到结束，基本上可以划分为如下 5 个阶段，如表 3.1 所示。



表 3.1　漏洞的生命周期

阶　段	事　件	描　述
第一阶段	系统漏洞被发现，并发布安全公告	由于软件设计者初期考虑不周等因素导致漏洞客观存在，漏洞研究人员发现漏洞并报告相关厂商，厂商向用户发布安全公告，并提供升级补丁程序
第二阶段	借助漏洞传播的病毒开始出现并传播	攻击者对安全补丁进行逆向工程，编写利用漏洞的攻击程序并发布但是用户在漏洞管理方面的疏忽，如没有在第一时间安装升级补丁程序，就会为蠕虫爆发创造条件，此阶段漏洞的危害较小
第三阶段	利用漏洞的蠕虫病毒大肆爆发	蠕虫在互联网上或者局域网利用系统漏洞大规模传播，导致网络堵塞或者瘫痪
第四阶段	系统漏洞被修复，但仍有发作	由于安装系统补丁，蠕虫丧失感染目标，已经感染的主机逐步清除使蠕虫源减少。少数没有安装补丁的主机数量减少，对网络的影响不大
第五阶段	漏洞影响逐渐消失	一段时间过后，由于系统升级或者完成系统补丁安装工作，或者使用新的软件版本，漏洞造成的影响逐步消失

3.1.3　漏洞管理流程

绝大部分的网络攻击都是借助目标网络的漏洞实现的。网络中的常规安全设备，如防火墙、入侵检测系统、UTM 等，很难阻止这种恶意攻击。要从根本上解决利用漏洞进行攻击的问题，就需要对漏洞产生的原因、漏洞的生命周期进行研究，同时配合人为的管理模式，建立行之有效的管理机制，并通过漏洞管理类的产品辅助执行漏洞管理。

1. 安全策略

安全策略是确保服务器、网络设备、客户端计算机以及网络安全设备能够正常工作的安全配置。大多数网络设备都可以提供丰富的安全功能，并且部分功能已经默认启用，用户可以根据实际需要，制定更加详细的安全策略。

2. 漏洞预警

漏洞预警工作通常由产品供应商完成，即确保在发现漏洞后，第一时间告知用户，如果没有相应的补丁程序，还应给出临时的解决方案等。这就要求漏洞管理产品的厂商应该有基础的漏洞研究、跟踪以及提供临时解决方案的能力。

3. 漏洞检测

执行检测工作之前需要对网络进行发现和跟踪，以便快速、准确地确定产生漏洞的计算机或网络设备。作为网络管理员，必须周期性的对网络中的网络资产进行检测，要求漏洞管理工具在保证一定的效率的前提下，具有较高的准确性。

注意

并不是检测到的漏洞越多越好，而是要对检测的有效性进行验证和分析。

4. 漏洞统计分析

漏洞检测完成后，需要通过具体的报告和数据对资产的风险进行评估和分析，清晰明了地显示出漏洞分布状况、详细描述以及相应的解决方案。

注意



要对网络中的资产风险进行分类，以便于对后续的漏洞修补工作进行优先级区分。这一过程也可以通过购买专业的漏洞管理设备或者安全服务来完成。

5. 漏洞修补

通过统计分析的结果指定切实可行的漏洞修补方案，并以合理的方式通知用户，例如通过自动更新服务器来提供最新的漏洞修补程序，用户可以按需下载，也可以由服务器自动分发完成。要注意补丁来源的合法性，以及补丁的安全性。通常情况下，必须对补丁程序进行小范围内安全性测试、兼容性测试后，确保补丁不会影响到业务系统的正常运行，才可以大范围分发。

6. 漏洞审计、跟踪

必须在网络中部署完善的漏洞审计机制，即对于新接入或启用的计算机或网络设备，进行补丁状态检测，如果不能满足安全要求，则拒绝继续访问，或通过其他措施使其可以获得所需的安全补丁。这个过程可以通过操作系统厂商、第三方的补丁管理软件或者专业的安全服务完成。

7. 其他问题

一个完善的漏洞管理机制能够有效地保证人为的管理疏漏不被攻击者利用，对于大多数利用漏洞的攻击会十分有效。网络管理人员在制定漏洞管理流程的时候，要根据实际情况进行细化或者裁减，确保漏洞管理的高效、灵活和实用。漏洞管理流程应该注意的其他问题包括：

- 工作流程标准化；
- 尽量使用专业的、自动化的漏洞管理工具，尽量避免人为操作；
- 尽量不要中断企业的业务流程，保证业务的正常运行；
- 漏洞修补尽量安排在晚上或者业务不繁忙的时候运行；
- 在测试环境中模拟测试通过，在确保不影响当前业务的状态下，实施漏洞修补工作流程；
- 针对不同的操作系统要准备不同的版本。

3.1.4 漏洞修补方略

大多数蠕虫病毒都是通过系统漏洞进行传播的，同时网络扫描和利用系统漏洞，也是“黑客”最常用的攻击手段之一。因此，做好网络的安全保障，必须做好漏洞补丁的安装管理工作。



对于个人用户而言，系统漏洞修补主要是安装官方网站发布的补丁，但是服务器或者网络中大规模部署补丁，通常是一项非常重要的工作。安装之前，必须先在实验环境中进行测试和分析，然后才可以在网络中大规模部署。

1. 环境分析

用户只有真正了解网络内部状况，才能有效地实施漏洞修补。例如，及时掌握网络资产情况、设备运行状态，包括网络运行的设备型号、厂商、操作系统种类及版本等。同时还要了解企业的主要业务系统及重要的数据，根据需要划分其安全等级，以确定补丁的紧急程度和修补时间。

2. 补丁分析

用户的计算机系统信息、硬件等的变化，都可能导致无法正确安装官方发布的系统漏洞补丁，甚至安装后还会导致一系列的问题。因此，部署之前一定要针对用户系统环境进行测试，切不可盲目的安装补丁，否则将带来许多意想不到的问题，其中包括：

- 导致系统兼容性出现问题，甚至不能使用；
- 系统崩溃，无法正常工作；
- 部分功能无法使用。

在得到补丁以后，正确的做法应该是：

- 在测试环境中，测试对业务系统的影响以及兼容性；
- 了解补丁自身的稳定性；
- 查看补丁是否还存在漏洞；
- 在大规模部署之前，进行小范围的短时间的联机测试。

在测试的过程中，应做好详细的测试记录，了解补丁程序和与其相关的组件对象之间的兼容性，对原有系统功能的影响，是否可以卸载，是否可以“回滚”等。

3. 分发安装

对于网络用户而言，管理员可以通过组策略、SMS、WSUS 等多种方法，将已获得的系统补丁分发到客户端。其中，WSUS 为微软公司提供的专用于补丁更新的服务组件，可以根据客户端实际情况，自动将补丁程序分发到用户的计算机中。

3.2　扫描隐藏的漏洞

漏洞扫描是网络安全防御中的一项重要技术，其原理是采用模拟攻击的形式对目标可能存在的已知安全漏洞进行逐项检查。其目标是工作站、服务器、交换机和数据库等，然后根据扫描结果向网络管理员提供周密可靠的安全性评估分析报告，从而为提高网络安全整体水平产生重要依据。

3.2.1 漏洞扫描概述

在网络安全体系的建设中，单机安全扫描是一种花费低、效果好、见效快、与网络运行相对独立、安装运行简单的工具，可以大规模减少网络管理员的手动劳动，有利于保持全网安全的统一和稳定。

目前，市场上有很多漏洞扫描工具，按照不同的技术（基于网络的、基于主机的、基于代理的、Client/Server）、不同的特征、不同的报告方法，以及不同的监听模式，可以分成很多种。不同的产品之间，漏洞检测的准确性差别较大，这就决定了生成报告的有效性上也有很大区别。选择正确的漏洞扫描工具，对于提高系统的安全性非常重要。

3.2.2 漏洞扫描的必要性

一般情况下，在网络边界处都会部署硬件或软件防火墙。防火墙作为不同网络或网络安全域之间信息的唯一出入口，能根据企业的安全政策控制（允许、拒绝、监测）出入网络的信息流，且本身具有较强的抗攻击能力。虽然防火墙是提供信息安全服务、实现网络和信息安全的基础设施，但是，它也存在着一定的局限性。

“外紧内松”是一般局域网络的特点，一道严密防守的防火墙其内部的网络也有可能防范松懈。

3.2.3 扫描工具的技术性能

采用漏洞扫描工具是保护系统安全的重要一步。当决定使用漏洞扫描以后，接下来的是如何选择满足企业需要的合适漏洞扫描软件或者工具。

选择扫描工具时，应当注意以下几个方面的问题：

- 漏洞库中的漏洞数量；
- 扫描工具的易用性；
- 是否可以生成漏洞报告，包括内容是否全面、是否可配置、是否可定制、报告的格式和输出方式等；
- 对于漏洞修复行为的分析和建议。是否只报告存在哪些问题、是否会告诉应该如何修补这些漏洞；
- 安全性。由于有些扫描工具不仅仅只是发现漏洞，而且还进一步自动利用这些漏洞，扫描工具自身是否会带来安全风险；
- 工具性能及价格。

3.3　漏洞扫描工具 MBSA

Microsoft Baseline Security Analyzer（MBSA）工具允许用户扫描一台或多台基于 Windows 的计算机，以发现常见的安全方面的配置错误。MBSA 将检查操作系统和已安装的其他组件（如：IIS 和 SQL Server），从而发现安全方面的配置错误，并及时通过推荐的安全更新进行修补。

3.3.1　扫描模式

MBSA 允许扫描一台或者多台计算机：

- 单台计算机。MBSA 最简单的运行模式是扫描单台计算机。默认情况下，将扫描本地计算机，管理员也可以通过指定计算机名或 IP 地址方式，使其扫描其他计算机。扫描远程计算机时，当前用户帐户必须拥有目标计算机的远程访问权限；
- 多台计算机。如果选择“选取多台计算机进行扫描”时，可以选择通过输入域名扫描整个域，或指定一个 IP 地址范围并扫描该范围内的所有基于 Windows 的计算机。

注意 
扫描远程单台主机或其他网段的计算机，必须使用具有相关权限的用户帐户。在进行“自动扫描”时，用来运行 MBSA 的帐户也必须是管理员或者是本地管理员组的成员。

3.3.2　扫描类型

MBSA 支持两种类型的扫描模式：

- MBSA 典型扫描。MBSA 典型扫描将执行扫描并且将结果保存在单独的 XML 文件中，这样就可以在 MBSA 查看器中进行查看，可以通过 MBSA GUI 方式（mbsa.exe）或 MBSA 命令行方式（mbsacli.exe）进行 MBSA 典型扫描，扫描内容包括所有可用的 Windows、IIS、SQL 和安全更新检查，每次执行 MBSA 典型扫描时，都会为每一台接受扫描的计算机生成一个安全报告，并保存正在运行 MBSA 的计算机中；
- HFNetChk 典型扫描。HFNetChk 典型扫描将只检查缺少的安全更新，并以文本的形式将扫描结果显示在命令行窗口中，与以前独立版本的 HFNetChk 处理方法完全相同，这种类型的扫描可以通过带有“/xmlout”开关参数（指示 MBSA 工具引擎进行 HFNetChk 扫描）的 mbsacli.exe 来执行。

3.3.3 查看安全报表

每次执行 MBSA 典型扫描时，都会为每一台接受扫描的计算机生成一个安全报表，并保存在正在运行 MBSA 的主机上。

安全报表默认的文件格式为 XML。可以按照计算机名、扫描日期、IP 地址或安全评估对这些报告进行排序。

3.3.4 网络扫描

MBSA 最多可以允许从服务器同时对 10 000 台计算机进行远程漏洞扫描。在防火墙或路由器将两个网络分开的多域环境中（两个单独的 Active Directory 域），TCP 的 139 端口和 445 端口以及 UDP 的 137 端口和 138 端口必须开放，以便 MBSA 连接和验证所要扫描的远程网络主机。

3.3.5 操作系统检查

MBSA 对在被扫描的计算机中 Windows 操作系统进行扫描，并检测是否存在以下漏洞。

1. 管理员组成员权限

该项检查将确定并列出属于本地管理员组的用户帐户。如果检测出的单个管理员帐户数量超过两个，则该工具将列出这些帐户名，并将该检查标记为一个潜在的安全漏洞。一般情况下，建议将管理员的数量保持在最低限度，因为管理员对计算机具有完全控制权。

2. 审核

该项检查将确定在被扫描的计算机上是否启用了系统审核功能。Windows 系统的审核特性，可跟踪和记录系统上的特定事件，如成功的和失败的登录尝试。通过监视系统的事件日志，可以发现潜在的安全问题和恶意活动。

3. 自动登录

该项检查将确定在被扫描的计算机上是否启用了“自动登录”功能，以及登录密码是否在注册表中以密文方式存储。如果“自动登录”已启用并且登录密码以明文形式存储，则安全报表就会将这种情况作为一个严重的安全漏洞反映出来。如果“自动登录”已启用而且密码以加密形式存储在注册表中，那么安全报表就会将这种情况作为一个潜在的安全漏洞标记出来。默认情况下，Windows Server 2008 禁止“自动登录”。

注意



如果扫描结果中提示“Error Reading Registry”（读取注册表时出错）消息，则表示远程注册表服务可能还未启用。



4. 自动更新

该项检查将确定是否在被扫描的计算机上启用自动更新功能，以及详细的配置情况。通常情况下，用户可以通过多种方式获取和安装更新，例如直接访问 Windows Update 站点、组策略远程部署、架设 WSUS 服务器等。当用户使用直接下载更新方式之外的其他方式时，扫描结果中可能会出现相关安全警告信息，提示自动更新没有正确配置，此时不必理会。

5. 域控制器

该项检查将确定正在接受扫描的计算机是否为域控制器，这主要是针对 Windows Server 2003 和 Windows Server 2008 系统而言的。在 Windows 域网络中，域控制器的地位和作用是非常重要的，不仅掌管着所有网络资源的安全访问，而且存储着所有网络用户的身份验证信息，如果存在安全漏洞，则后果不堪设想。基于上述原因，域控制器应该被视为需要加强保护的关键资源。应确认当前网络是否需要将这台计算机作为域控制器，并确认是否采取了相应的步骤来加强这台计算机的访问安全。

6. 文件系统

该项检查将确定在每个分区使用的文件系统类型。NTFS 具有访问控制功能，是一个安全的文件系统，因此，服务器所有分区均使用该文件系统，如果使用 FAT32 文件系统，则扫描结果中将报警。

注意



为了使该检查成功执行，驱动器必须通过管理驱动器共享来实现共享。

7. 来宾帐户

该项检查将确定在被扫描的计算机上是否启用了系统内置的来宾帐户。来宾帐户主要是为临时用户提供的，默认情况下是禁用的。当用户在计算机或域上没有帐户，或者在计算机所在的域信任的任何一个域中没有帐户时，可以使用这种帐户登录到 Windows Server 2008 系统的计算机。

如果在 Windows Server 2008 计算机上已启用来宾帐户，则此时将在安全报表中作为一个安全漏洞标记出来。如果在使用简单文件共享的 Windows XP 计算机上已启用来宾帐户，则这种情况将不会作为安全漏洞标记出来。

8. 本地帐户密码

该项检查将找出使用空白密码或简单密码的所有本地用户帐户。Windows 2000/XP/2003 系统的管理员帐户密码均可以设置为空，因此存在很大的安全隐患。在 Windows Server 2008 系统中，必须设置符合相应复杂程度的安全密码，才允许启用管理员帐户。因此该项扫描只适用于 Windows 2000/XP/2003 系统，如果本地用户帐户密码符合下列条件之一，就会出现警告：

- 密码为空白；
- 密码与用户帐户名相同；

- 密码与计算机名相同；
- 密码使用“password”一词；
- 密码使用“admin”或“administrator”一词。

提示　该项检查可能会花较长时间，这取决于计算机上的用户帐户数量。因此，管理员可能想要在扫描他们所在网络的域控制器前禁用该检查。

---

9. 密码过期

该项检查将确定是否有本地用户帐户设置了永不过期的密码。密码应该定期更改，以降低遭到密码攻击的可能性。

10. 限制匿名用户

该项检查将确定被扫描的计算机上是否使用了 RestrictAnonymous 注册表项来限制匿名连接。允许匿名连接本身就是一个很危险的系统漏洞，何况匿名用户还可以列出某些类型的系统信息，其中包括用户名及其详细信息、帐户策略和共享名，因此必须对安全要求严格的服务器限制此项功能，以使匿名用户无法访问。

11. 共享资源

该检查将确定在被扫描的计算机上是否存在共享文件夹。扫描报告将列出在计算机上发现的所有共享内容，其中包括管理共享及其共享级别和 NTFS 级别的权限。通常情况下，应关闭系统中非必要的共享目录，尤其是服务器更应如此。扫描结果中将列出所有的系统默认共享，和用户后期设置的重要资源共享。

12. Windows 防火墙

该项检查将确定是否在被扫描的计算机上对所有的活动网络连接启用 Windows 防火墙，这主要是针对 Windows Server 2008 系统而言的。如果已经启用防火墙，则还将对其开放的入站端口进行检测。如果上述系统的 Windows 防火墙没有开启，或者开放了存在安全漏洞的端口，则扫描结果中将出现警告信息。

13. 检查是否存在不必要的服务

该检查将确定被扫描计算机上的 services.txt 文件中，是否包含有已启用的服务。services.txt 文件是一个可配置的服务列表，这些服务都不应该在被扫描的计算机上运行。此文件由 MBSA 安装并存储在该工具的安装文件夹中。该工具的用户应配置 services.txt 文件，以便包括在各台被扫描的计算机上所要检查的那些特定服务。默认情况下，与该工具一起安装的 services.txt 文件包含下列服务：

- MSFTPSVC（FTP）；
- TlntSvr（Telnet）；
- W3SVC（WWW）；
- SMTPSVC（SMTP）。

服务是一种程序，只要计算机在运行操作系统，其就在后台运行。服务不要求用户必须进行登录。服务用于执行不依赖于用户的任务，如等待信息传入的传真服务。

3.3.6　IIS 漏洞检查

如果目标计算机上安装了 IIS 服务，则 MBSA 还可以扫描 IIS 程序或设置上存在的漏洞，包括以下 7 种。

1. MSADC 和脚本虚拟目录

该项检查将确定 MSADC（样本数据访问脚本）和脚本虚拟目录，是否已安装在被扫描的计算机上。这些目录通常包含一些非必要的脚本文件，将其删除可缩小计算机受攻击的范围。

2. SADMPWD 虚拟目录

该检查将确定 IISADMPWD 目录是否已安装在被扫描的计算机上。IIS 4.0 能让用户更改他们的 Windows 密码并通知用户密码即将到期。IISADMPWD 虚拟目录包含了此功能所要使用的文件，在 IIS 4.0 中，IISADMPWD 虚拟目录将作为默认 Web 站点的组成部分进行安装。此功能是作为一组.htr 文件和一个名为 Ism.dll 的 ISAPI 扩展加以实现的，.htr 文件位于\System32\Inetsrv\Iisadmpwd 目录中。

3. 域控制器上的 IIS

该检查将确定 IIS 是否在一个作为域控制器的系统上运行。这种情况将在扫描报告中作为一个严重安全漏洞加以标记，除非被扫描的计算机是一台小型企业服务器（Small Business Server）。

建议不要在域控制器上运行 IIS Web 服务器。域控制器上有敏感的数据（如用户帐户信息），不应该用作另一个角色。如果在一个域控制器上运行 Web 服务器，就增加了保护服务器安全和防止攻击的复杂性。

4. IIS 锁定工具

该项检查将确定 IIS Lockdown 工具（Microsoft Security Tool Kit 的一部分）是否已经在被扫描的计算机上运行。IIS Lockdown 工具的工作原理是，关闭 IIS 中不必要的功能，从而缩小攻击者可以利用的攻击面。

自从 Windows Server 2003 的 IIS 6.0 开始，就已经不再需要 IIS Lockdown 工具，默认情况下已经锁定了相关功能。对于从 IIS 4.0 安装升级到 IIS 6.0 或 IIS 7.0 的，则应该使用 IIS Lockdown 来确保仅在服务器上启用了所需的服务。

5. IIS 日志记录

该项检查将确定 IIS 日志记录功能是否已启用，以及是否已使用了 W3C 扩展日志文件格式。

Windows 的事件日志记录中，没有包括 IIS 日志记录。IIS 日志记录通常包括站点运行状态的详细情况，如哪些用户访问过该站点、浏览内容、时间等。管理员可以根据需要选择对任

何站点、虚拟目录或文件进行审核，通过定期复查审核结果，可以检测到服务器或站点中可能遭受攻击或其他安全问题的方面。在启用了日志记录之后，也就对该站点的所有文件夹启用了日志记录，但也可以对特定的目录禁用日志记录。

6. IIS 父路经

该项检查将确定在被扫描的计算机上，是否启用了 ASPEnableParentPaths 设置。通过在 IIS 上启用父路经，Active Server Page（ASP）页就可以使用到当前目录的父目录的相对路径。

7. IIS 样本应用程序

该项检查将确定下列 IIS 示例文件目录是否安装在计算机上：

\Inetpub\iissamples

\Winnt\help\iishelp

\Program Files\common files\system\msadc

通常与 IIS 一起安装的样本应用程序会显示动态 HTML（DHTML）和 Active Server Pages（ASP）脚本，并提供联机文档。

3.3.7　SQL 检查

MBSA 可以对在被扫描计算机中 SQL Server 和 MSDE 的所有实例进行扫描，并检测是否存在以下漏洞。

1. Sysadmin 角色的成员

该项检查将确定 Sysadmin 角色的成员数量，并将结果显示在安全报表中。

SQL Server 角色将具有相同操作权限的登录帐户组合到一起，对于固定的服务器角色，Sysadmin 将系统管理员权限提供给其所有成员。

注意



如果扫描结果中显示“No permissions to access database（无权访问数据库）”错误消息，则可能没有访问 MASTER 数据库的权限。

2. 将 CmdExec 权限授予 Sysadmin

该项检查将确保 CmdExec 权限仅被授予 Sysadmin，其他所有具有 CmdExec 权限的帐户都将在安全报表中列出。

SQL Server 代理是 Windows NT/2000/XP/Vista 系统中的一项服务，负责执行作业、监控 SQL Server 和发送警报。通过 SQL Server 代理，可以使用脚本化作业步骤使某些管理任务实现自动化。作业是 SQL Server 代理按顺序执行的一个指定的操作序列，一项作业可以执行范围广泛的活动，其中包括运行 Transact-SQL 脚本、命令行应用程序和 Microsoft ActiveX 脚本。用户可以创建作业，以便运行经常重复或者计划的任务，而作业也可以通过生成警报自动将它们的状态通知给用户。

3. SQL Server 本地帐户密码

该项检查将确定是否有本地 SQL Server 帐户采用了简单密码。这一检查将列举所有用户帐户并检查是否有帐户使用下列密码：

- 密码为空白；
- 密码与用户帐户名相同；
- 密码与计算机名相同；
- 密码使用“password”一词；
- 密码使用“sa”一词；
- 密码使用“admin”或“administrator”一词。

4. SQL Server 身份验证模式

该项检查将确定被扫描的 SQL Server 使用的身份验证模式。Microsoft SQL Server 为提高对该服务器进行访问的安全性提供了两种模式：Windows 身份验证模式和混合模式。

在 Windows 身份验证模式下，Microsoft SQL Server 只依赖 Windows 系统对用户进行身份验证。然后，Windows 用户或组就得到授予访问 SQL Server 的权限。在混合模式下，用户可能通过 Windows 或通过 SQL Server 进行身份验证。经过 SQL Server 身份验证的用户将用户名和密码保存在 SQL Server 内。Microsoft 强烈推荐始终使用 Windows 身份验证模式。

5. Windows 身份验证模式

该安全模式使 SQL Server 能够像其他应用程序，依赖于 Windows 对用户进行身份验证。使用此模式与服务器建立的连接叫作受信任连接。当使用 Windows 身份验证模式时，数据库管理员通过授予用户登录到 SQL Server 的权限来允许他们访问运行 SQL Server 的计算机。Windows 安全识别符（SID）将用于跟踪使用 Windows 进行身份验证的用户。在使用 Windows SID 的情况下，数据库管理员可以将访问权直接授予 Windows 用户或组。

6. 混合模式

在 SQL Server 中，当客户端和服务器都可以使用 NTLM 或 Kerberos 登录身份验证协议时，混合模式将依赖 Windows 对用户进行身份验证。如果其中某一方不能使用标准 Windows 登录，那么 SQL Server 就会要求提供用户名和密码，并将用户名和密码与存储在其系统表中的用户名和密码进行比较。依赖用户名和密码建立的连接叫作不受信任的连接。

之所以提供混合模式，有以下两方面原因：

- 向后兼容 SQL Server 的旧版本；
- 在 SQL Server 安装到 Windows 9x 操作系统时实现兼容。

7. Sysadmin 角色中的 SQL Server BUILTIN\Administrators

该项检查将确定 Administrators 组是否被列为 Sysadmin 角色的成员。

> 注意　如果扫描结果中显示“No permissions to access database”（无权访问数据库）错误消息，则可能不具有访问 MASTER 数据库的权限。

SQL Server 角色是一个安全帐户，同时也是包含了其他安全帐户的一个帐户集合。进行权限配置时，可以将其看成一个单独的单元。一个角色可以包含 SQL Server 登录权限、其他角色和 Windows 用户帐户或组。

固定的服务器角色具有涵盖整个服务器的作用域，这些角色存在于数据库外部。一个固定服务器角色的每个成员，都能够向相同角色中添加其他登录。默认情况下，Windows BUILTIN\Administrators 组（本地管理员的组）的所有成员都是 Sysadmin 角色的成员，从而向其赋予了对所有数据库的完全访问权。

8. SQL Server 目录访问

该项检查将验证下列 SQL Server 目录是否都只将访问权授予 SQL 服务帐户和本地管理员：

- Program Files\Microsoft SQL Server\MSSQL$InstanceName\Binn
- Program Files\Microsoft SQL Server\MSSQL$InstanceName\Data
- Program Files\Microsoft SQL Server\MSSQL\Binn
- Program Files\Microsoft SQL Server\MSSQL\Data

该工具将扫描这些文件夹中每个文件夹上的访问控制列表，并列举出列表中包含的用户。如果任何其他用户（除 SQL 服务帐户和管理员以外）具有读取或修改这些文件夹的访问权，则该工具将在安全报表中将此检查标记为一个安全漏洞。

9. SQL Server 公开的 SA 帐户密码

该项检查将确定 SQL Server 的 SA 帐户密码是否以明文形式写入日志文件中。在 SQL Server 2000/2005 中，如果域凭证用于启动 SQL Server 服务，也会检查日志文件。如果在设置 SQL Server 时使用混合模式身份验证，则 SA 密码以明文形式保存；如果使用 Windows 身份验证模式，管理员选择提供自动启动 SQL Server 服务时使用的域凭证，只会使凭证处于危险境地。

10. SQL Server 来宾帐户

该项检查将确定 SQL Server 来宾帐户是否具有访问数据库（Master、tempdb 和 msdb 除外）的权限。该帐户具有访问权的所有数据库都将在安全报表中列出。



> 注意　如果扫描结果中显示“No permissions to access database”（无权访问数据库）错误消息，则可能不具有访问 MASTER 数据库的权限。

在 SQL Server 中，一个用户登录帐户必须以下列方式之一获得访问数据库及其对象的授权。

- 登录帐户可以被指定为一个数据库用户；
- 登录帐户可以使用数据库中的来宾帐户；
- Windows 组登录可以映射到一个数据库角色。然后，属于该组的单个 Windows 帐户都可以连接到该数据库。



db_owner 或 db_accessadmin 数据库角色的成员或者 Sysadmin 固定服务器角色成员，都可以创建数据库用户帐户角色。一个帐户可以有多个参数：SQL Server 登录 ID、数据库用户名和角色名称。数据库用户名称可以与用户的登录 ID 不同。如果未提供数据库用户名，则该用户的登录 ID 和数据库用户名完全相同。创建数据库用户后，可以根据需要为该用户分配任意数量的角色。如果未提供角色名称，则该数据库用户只是公共角色的一个成员。

db_owner、db_accessadmin 或 Sysadmin 角色的成员还可以创建来宾帐户，来宾帐户允许任何合法的 SQL Server 登录帐户访问数据库。默认情况下，来宾帐户将继承分配给公共角色的所有特权；不过，这些特权可以被更改，使其权限大于或小于公共角色特权。

11. 域控制器上的 SQL Server

该检查将确定 SQL Server 是否运行域控制器上。域控制器包含有敏感数据，通常不再用来提供其他网络服务。如果在域控制器上运行 SQL Server，则增加了保护服务器安全和防止攻击的复杂性，建议不要这样部署。

12. SQL Server 注册表项安全

该项检查将确保 Everyone 组对下列注册表项的访问权被限制为读取权限：

- HKLM\Software\Microsoft\Microsoft SQL Server
- HKLM\Software\Microsoft\MS SQLServer

如果 Everyone 组对这些注册表项的访问权限高于读取权限，则这种情况将在安全扫描报告中被标记为严重安全漏洞。

13. SQL Server 服务帐户

该检查将确定 SQL Server 服务帐户在被扫描的计算机上是否为本地或域管理员组的成员，或者是否有 SQL Server 服务帐户正在 LocalSystem 上下文中运行。

在被扫描的计算机上，MSSQLServer 和 SQLServerAgent 服务帐户都要经过检查。

注意

如果扫描结果中显示“No permissions to access database”（无权访问数据库）错误消息，则可能不具有访问 MASTER 数据库的权限。

3.3.8　桌面应用程序检查

MBSA 对在被扫描的计算机中桌面应用程序进行扫描，并检测是否存在以下漏洞：

1. IE 安全区域

该项检查将列出被扫描计算机上所有本地用户当前采用的 IE 区域安全设置，并给出合理建议。

IE 内容区域将 Internet 或 Intranet 分成具有不同安全级别的区域。对于每个安全区域，可

以选择相应的安全级别，或者自定义安全设置。Microsoft 建议，对于不能确定是否可信任的区域内的站点，应将安全性设置为高。自定义选项为高级用户和管理员提供了针对所有安全选项的更多的控制权，其中包括下列几项：

- 对文件、ActiveX 控件和脚本的访问；
- 提供给 Java 小程序的功能级别；
- 带有安全套接字层（SSL）身份验证的站点身份指定；
- 带有 NTLM 身份验证的密码保护（根据服务器所在的区域，Internet Explorer 可以自动发送密码信息，提示用户输入用户和密码信息，或者干脆拒绝任何登录请求）。

2. 面向管理员的 IE 增强安全配置

该检查可识别出运行 Windows Server 2008 的计算机上，是否已经启用针对管理员的 IE 增强安全配置（Enhanced Security Configuration）。如果已经安装了针对管理员的 IE 增强安全配置，这一检查还会识别出禁用该 IE 增强安全配置的管理员。

3. 面向非管理员的 IE 增强安全配置

该检查识别出在运行 Windows Server 2008 的计算机上，是否已经启用用于非管理员用户的 Internet Explorer 增强安全配置（Enhanced Security Configuration）。如果已经安装了针对非管理员的 Internet Explorer 增强安全配置，这一检查还会识别出禁用该 Internet Explorer 增强安全配置的非管理员用户。

4. Office 安全配置和分析宏保护

该检查将对每个用户逐一确定 Microsoft Office 2007/2003/2000/97 宏保护的安全级别。MBSA 还将对 PowerPoint、Word、Excel 和 Outlook 进行检查。

宏能够将重复的任务自动化。这样可以节省时间，但也会被用于传播病毒，例如当用户打开包含恶意宏的受感染文档时，会使恶意宏蔓延到系统上的其他文档，或者传播给其他用户。

3.4 修补系统漏洞的原则

修补系统漏洞是发现漏洞后的第一要务。产品供应商发现漏洞之后，会在最短的时间内发布对应的修补程序，用户可以免费获取、安装，使系统恢复到安全状态。看似简单的过程，却暗含着许多用户需要注意的事项。通常情况下，不同类型的产品、不同的应用环境，都必须选择适用的补丁程序，否则不仅起不到修补作用，还可能导致新的漏洞，甚至造成系统崩溃的严重后果。

3.4.1　备份相关数据

在安装补丁之前，最好将相关的文件进行备份，以免造成错误，丢失重要数据或者导致系统无法正常运行。如果是针对操作系统的补丁，则应确保补丁具备“回滚”功能。

通常情况下，需要备份的数据包括两部分：

- 原来程序的安装目录。对于绿色软件而言，只需备份相应的目录即可；
- 系统的 DLL 动态库文件。查明可能覆盖的相关的 DLL 文件并单独备份，如果安装补丁时由于覆盖 DLL 文件，导致系统故障，则可以进入安全模式，将备份的 DLL 文件重新覆盖相关的 DLL 文件即可。

3.4.2　核对补丁信息

用户可以通过多种渠道获得漏洞补丁程序，但是需要注意的是，这些补丁通常都是针对特定产品的，安装之前必须仔细阅读相关信息。

1. 阅读补丁声明

在运行补丁程序之前，一定要仔细阅读有关的说明文档，充分了解补丁的功能、用法、对应漏洞的情况，对安装补丁后发生的后果要做到心中有数。然后根据企业的网络环境进行分析，判断可能产生的风险，根据漏洞的紧急情况，判断是否需要安装补丁。需要提前做好预备工作，确保针对在补丁安装完成后出现的问题，能有高效、快捷、安全的补救措施。

2. 对号下载补丁

注意补丁程序对应的操作系统和应用软件的版本。很多补丁都是针对某个特定的操作系统和应用软件版本而开发的。除此之外，使用时还要下载与操作系统（还要注意不同语言版本）、应用程序匹配的补丁程序。

3. 下载安全补丁

补丁的来源一定要安全，必须到可靠的平台下载，或者到有安全认证的供应商那获取相关的补丁程序，防止被恶意修改或安装了嵌入“木马”的补丁。建议到官方的网站和信誉较好的网站下载补丁安装或者在线安装补丁，一方面可以保证下载的补丁是安全有效的，另一方面可以保证补丁安装包的时效性。

3.4.3　选择安装模式

通常情况下，补丁的安装有在线安装和下载结束再安装这两种模式，可以根据企业的网络状况选择适合自己的安装模式。如果网络环境稳定，可以选择在线安装，否则建议将补丁下载

到本地在进行安装，可以有效避免因为网络原因（线路故障等）造成的安装失败。

在补丁安装的时候，要退出正在运行的应用程序，否则可能会出现因为文件正在使用无法正常安装补丁的情况。对于系统启动加载的应用程序，尽量将其从启动项中删除再进行补丁的安装。

总之，部署补丁时，一定要注意补丁的安装策略，否则事与愿违，给工作带来不必要的麻烦。

3.5 微软免费修补漏洞工具

软件和系统漏洞问题一直困扰着广大计算机用户，对于这些漏洞所带来的隐患，也只有通过及时下载补丁来预防。对绝大多数用户来说，选择一款好用的漏洞修补工具是非常重要的，而 Windows 系统自身带有漏洞修补更新工具，更是帮助用户解决了漏洞修补功能。

3.5.1 用 Microsoft Update 安装补丁

Microsoft Update 是微软公司发布所有产品漏洞补丁的官方网站，Windows Server 2008 用户，可以直接使用系统自带的 Windows Update 向导，完成 Windows 系统及其他 Microsoft 产品的自动更新。

1. 安装系统更新

更新是软件的添加项，有助于防止问题或修复问题、改进计算机的工作方式、增强计算机性能。使用自动更新，无须联机搜索更新，也无须担心计算机缺少 Windows 的关键修复程序。Windows 会自动检查适用于计算机的最新更新。

01 启动 Windows Server 2008 系统，依次选择“开始”→“所有程序”→“Windows Update”选项，打开“Windows Update”窗口。单击“现在安装”按钮，开始下载更新，完成后显示如图 3.1 所示结果。

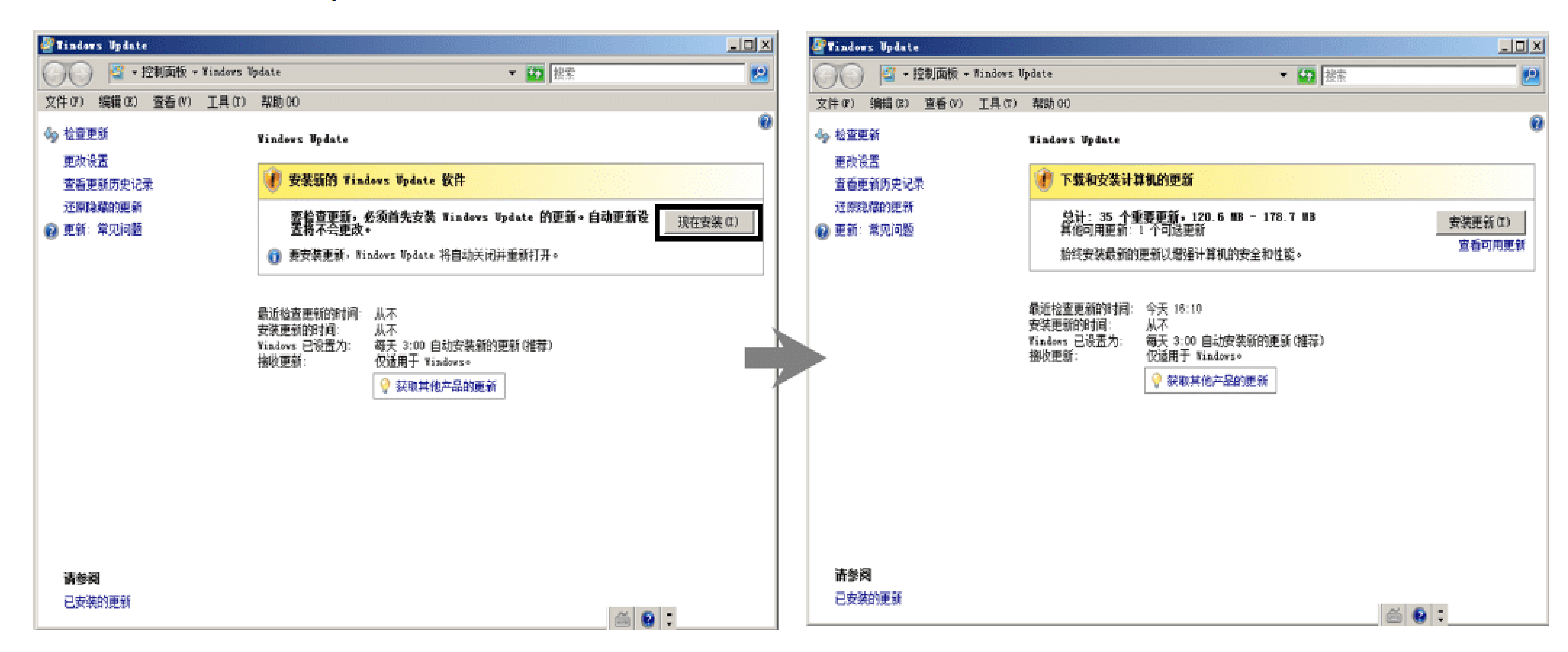


图 3.1 下载和安装计算机的更新

02 单击“安装更新”按钮，显示如图 3.2 所示“Windows Update”对话框，从微软的网站下载计算机更新程序。

03 选中“我接受许可条款”单选按钮，单击“完成”按钮，返回如图 3.3 所示“Windows Update”窗口，显示正在下载更新。



图 3.2　检测更新



图 3.3　正在下载更新

04 更新完成后，单击“立即重新启动”按钮以完成安装更新。

2. 查看更新历史记录

更新完成后，用户可以对系统更新的历史记录进行查看。

01 打开“Windows Update”窗口，在左侧窗格中，单击“查看更新历史记录”链接，打开如图 3.4 所示“查看更新历史记录”窗口。

02 可以查看所有历史的系统更新记录。

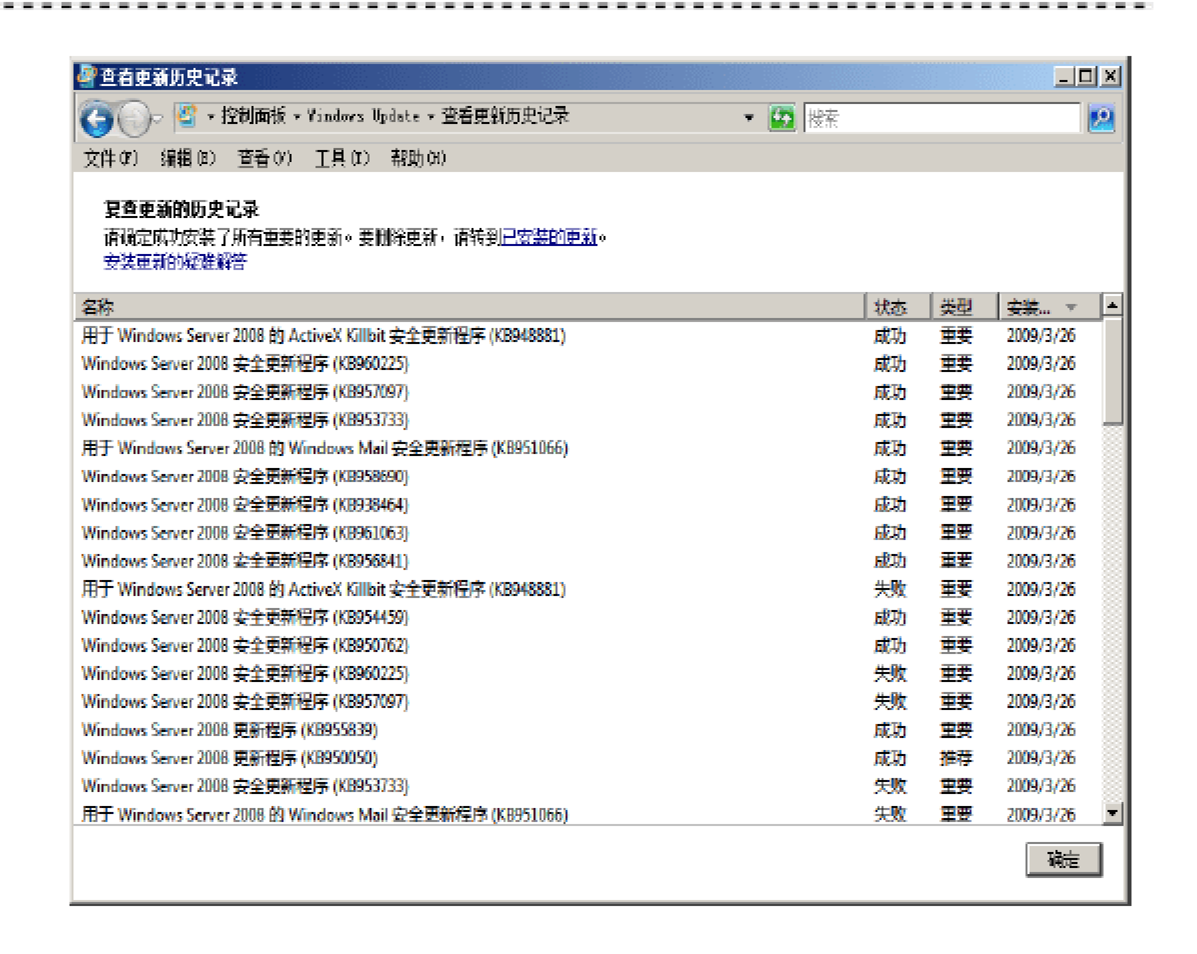


图 3.4　“查看更新历史记录”窗口

3.5.2　系统更新服务

WSUS（Windows Software Update Service）是个微软推出的免费的网络化补丁分发方案，可以从微软网站中下载获得。WSUS 支持微软公司全部产品更新，使信息技术管理员能够将最新的 Microsoft 产品更新部署至计算机上。

1. WSUS 概述

通常情况下，家庭或中小型用户都是直接从 Microsoft Update 服务器直接下载所需更新程

序。但是，如果在大型网络中，仍然使用这种方式，每天仅此一项网络流量就可能占去一大部分。而通过 WSUS 这个内部网络中的 Windows 升级服务，就让所有 Windows 更新都集中下载到内部网的 WSUS 服务器中，使网络中的客户机通过 WSUS 服务器得到更新。这在很大程度上节省了网络资源，避免了外部网络流量的浪费并且提高了内部网络中计算机的更新效率，WSUS 的体系结构如图 3.5 所示。

如果网络规模比较大，还可以采用“多级”WSUS 结构，如图 3.6 所示。其中，“上游 WSUS 升级服务器”负责从 Microsoft Update 站点下载升级补丁并管理下游的 WSUS 升级服务器，“下游”的升级服务器从“上游”升级服务器获得补丁，并为企业网络中的工作站提供升级补丁。所有的工作站被划分到不同的“下游升级服务器”中并且从其设置的“下游”升级服务器获得补丁。

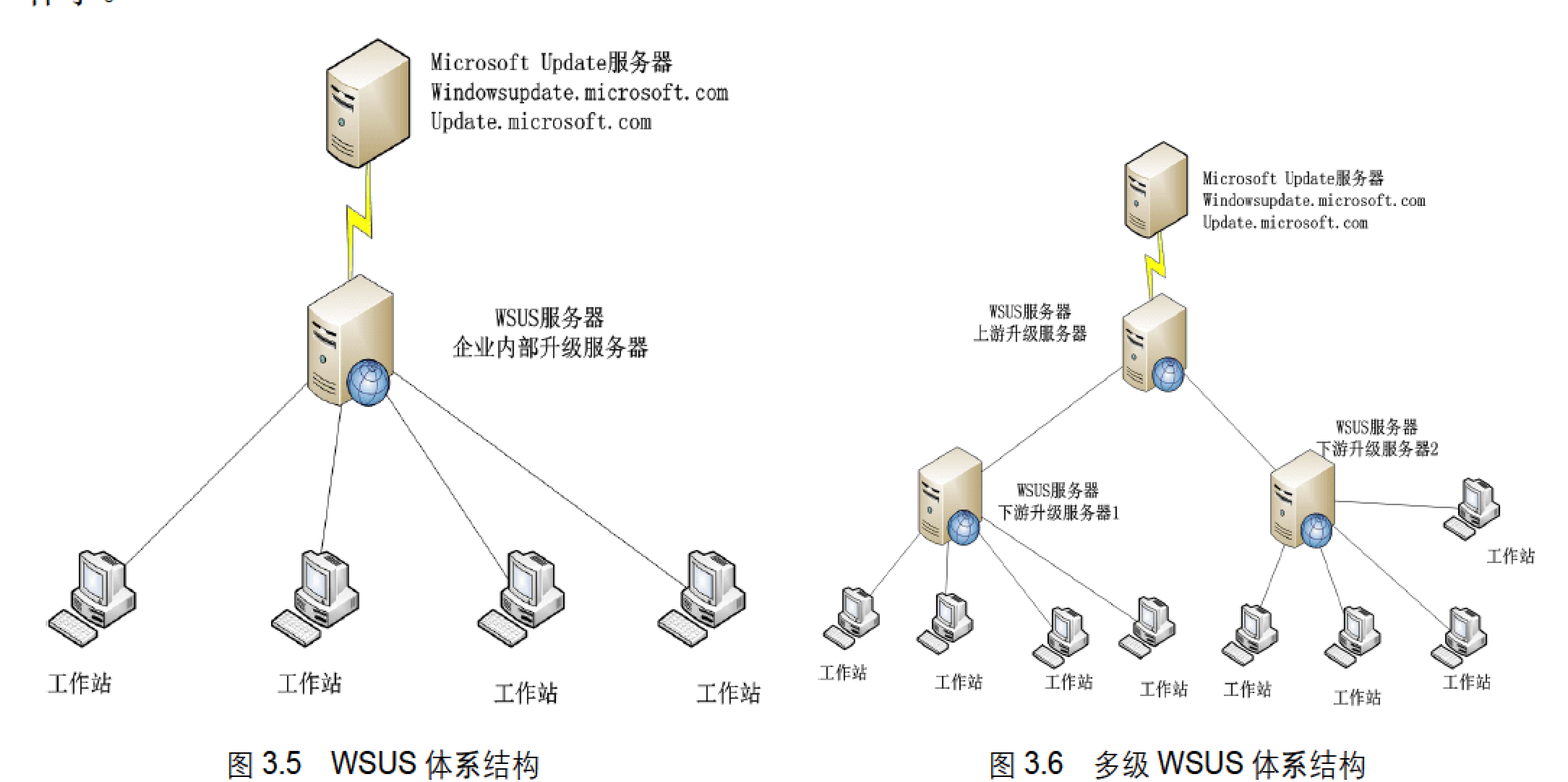


图 3.5 WSUS 体系结构　　图 3.6 多级 WSUS 体系结构

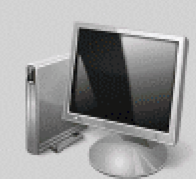
2. 配置 WSUS 服务器

WSUS 是一款服务器/客户端模式的软件，应用之前应先正确配置服务器端。安装 WSUS 服务器时，必须使用具有本地管理员权限的用户帐户登录系统。另外，如果安装完成后想立即启动 Web 管理工具，还必须为 Administrator 用户帐户设置不为空的登录密码。

（1）软件需求

WSUS 3.0 SP1 对操作系统版本、操作系统上运行的服务、IIS、数据库、磁盘分区格式、硬盘可用空间都有一定的要求：

- WSUS 服务器系统平台可以是 Windows Server 2003 SP1/SP2、Windows Server 2003 R2 或 Windows Server 2008；
- 目标服务器不能安装“终端服务”，如果确认需要使用“终端服务”对计算机管理管理，则可以在安装 WSUS 之前临时将其删除。安装 WSUS 后，重新安装“终端服务”即可；
- WSUS 3.0 SP1 需要 IIS 6.0/7.0 的支持。如果服务器是从 Windows Server 2000 升级到 Windows Server 2003 的，则默认情况下，IIS 可能在 IIS 5.0 兼容模式下运行，这也可能会导致安装失败；



- WSUS 根服务器必须可以连接到 Internet，如果使用代理服务器连接 Internet，则代理服务器必须支持 HTTP 或者 HTTPS 方式；
- 安装 WSUS 时，需要禁止正在运行的防病毒程序和一切防火墙软件；
- 如果在网络中配置需要协同工作的多台 WSUS 服务器，则需要安装专用的 SQL Server 2005 数据库，安装程序默认安装的 WMSDE 数据库只能用于独立的 WSUS 服务器；
- 如果安装 WSUS 的服务器操作系统为 Windows Server 2008，则满足操作系统需求即可，如果是 Windows Server 2003 系统，则除满足系统运行需求外，必须确保内存不低于 512M。

（2）硬件需求

WSUS 3.0 SP1 功能虽然有了明显提升，但硬件需求方面变化不大。以下是客户端数量不大于 500 个的 WSUS 服务器的主要硬件配置信息：

- 服务器内存至少为 1 GB；
- 处理器至少为 1 GHz 或更高；
- 磁盘空间依据所选数据库的不同而有所区别，建议保留 30 GB 的自由空间用于存储下载数据和数据库信息；
- 确保 WSUS 服务器到 Internet 以及和客户端之间的网络连接正常。

（3）准备工作

在即将安装 WSUS 的计算机上，安装 Windows Server 2008 系统及各种驱动程序，配置网卡的 IP 地址、子网掩码、网关及 DNS 等参数，使其可以连接到 Internet，如果通过代理服务器连接到 Internet，则应指定正确的代理服务器信息和有效身份凭证。安装 WSUS 之前应做好如下准备工作：

- 安装 IIS 服务；
- 后台智能传输服务（BITS）2.0；
- Report Viewer（可选组件，建议安装）。

注意



安装 IIS 过程中，应确保以选择“应用程序开发”中的“ASP .NET 组件”，否则将无法完成 WSUS 安装。

（4）安装 WSUS 服务器

用户可以登录以下站点免费获取最新版的 WSUS 服务器安装文件，一切准备工作就绪之后即可开始安装 WSUS 服务器，具体安装过程如下。

01 将下载的安装包解压缩至本地计算机的某个目录下，执行其中的 WusSetup.exe 文件即可启动 WSUS 安装向导，依次单击“下一步”按钮，选择安装模式、接受许可协议和设置本地存储更新的目录，如图 3.7 所示。在“安装模式选择”对话框中，选择“包括管理控制台的完整服务器安装”单选按钮。设置为本地存储更新时，需要确保所选分区的可用磁盘空间足够大。



图 3.7　设置安装模式和更新源

02 依次单击“下一步”按钮，设置数据库类型和使用的 Web 站点，如图 3.8 所示。在“数据库选择”对话框中，选择“在此计算机上安装 Windows Internal Database”单选按钮，并指定保存 WSUS 数据库文件的位置。WSUS 数据库中存储的信息包括：WSUS 服务器配置信息、用于描述更新程序作用的元数据和客户端计算机、更新程序信息以及客户端计算机所进行的更新情况，通常不会占用太多空间。在“网站选择”对话框中，选择“使用现有 IIS 默认网站”单选按钮，即可使用系统默认的 80 端口，作为此站点的通信端口；如果当前服务器上存在正在运行的 Web 站点，且已占用 80 端口，则可以选择“创建 Windows Server Update Services 3.0 SP1 网站”单选按钮，使用 8530 端口创建用于 WSUS 管理的 Web 站点。

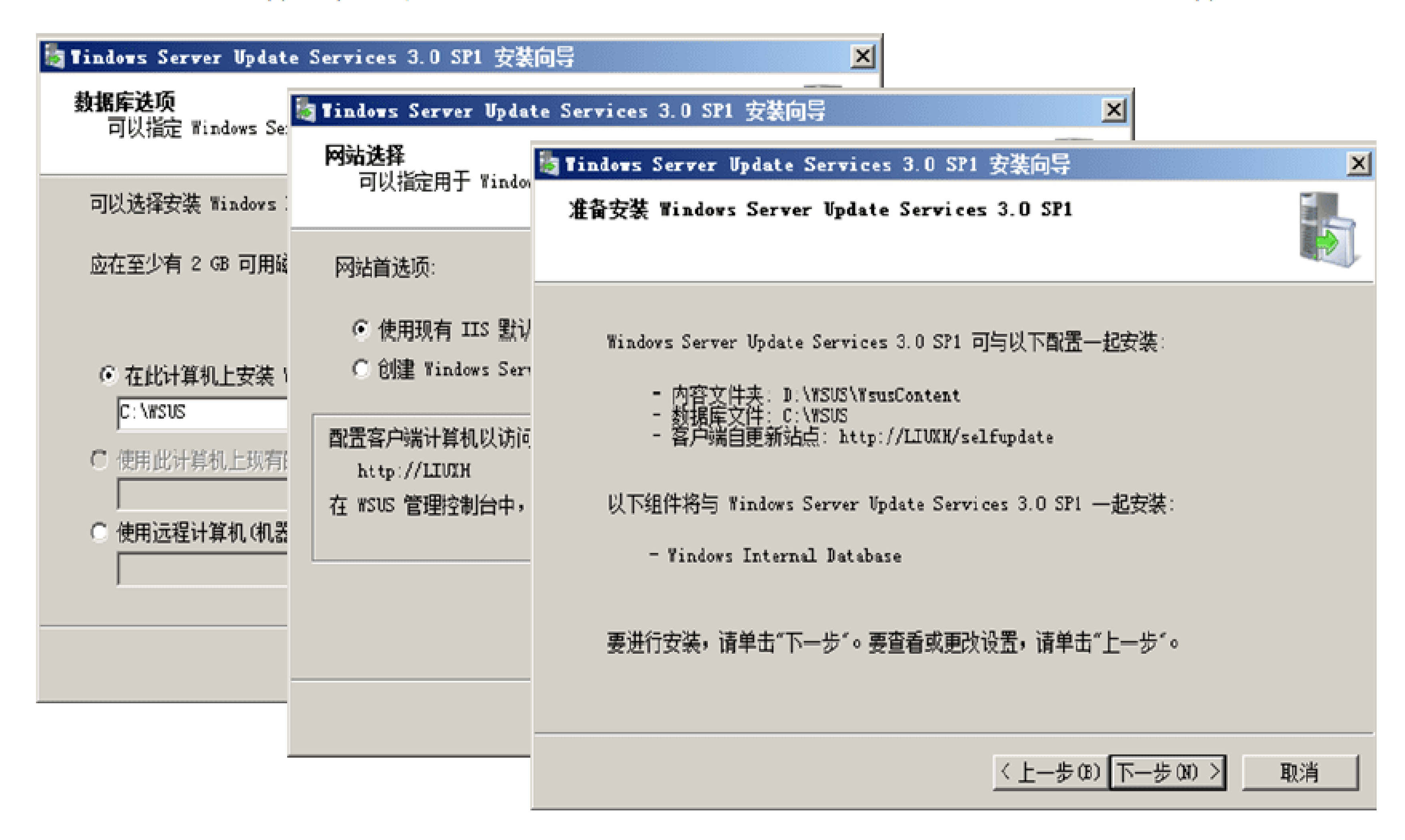


图 3.8　设置数据库和站点

提示



WSUS 还可以使用本地或远程计算机上的 SQL Server 2000/2005 数据库，但需要注意的是 WSUS 只支持 Windows 认证。如果是独立的 WSUS 服务器，则建议使用其默认的数据库。

03 安装完成后，将自动关闭 Windows Server Update Services 3.0 SP1 安装向导，同时显示如图 3.9 所示“Windows Server Update Services 配置向导”对话框，通过向导即可配置 WSUS 服务器的相关选项。



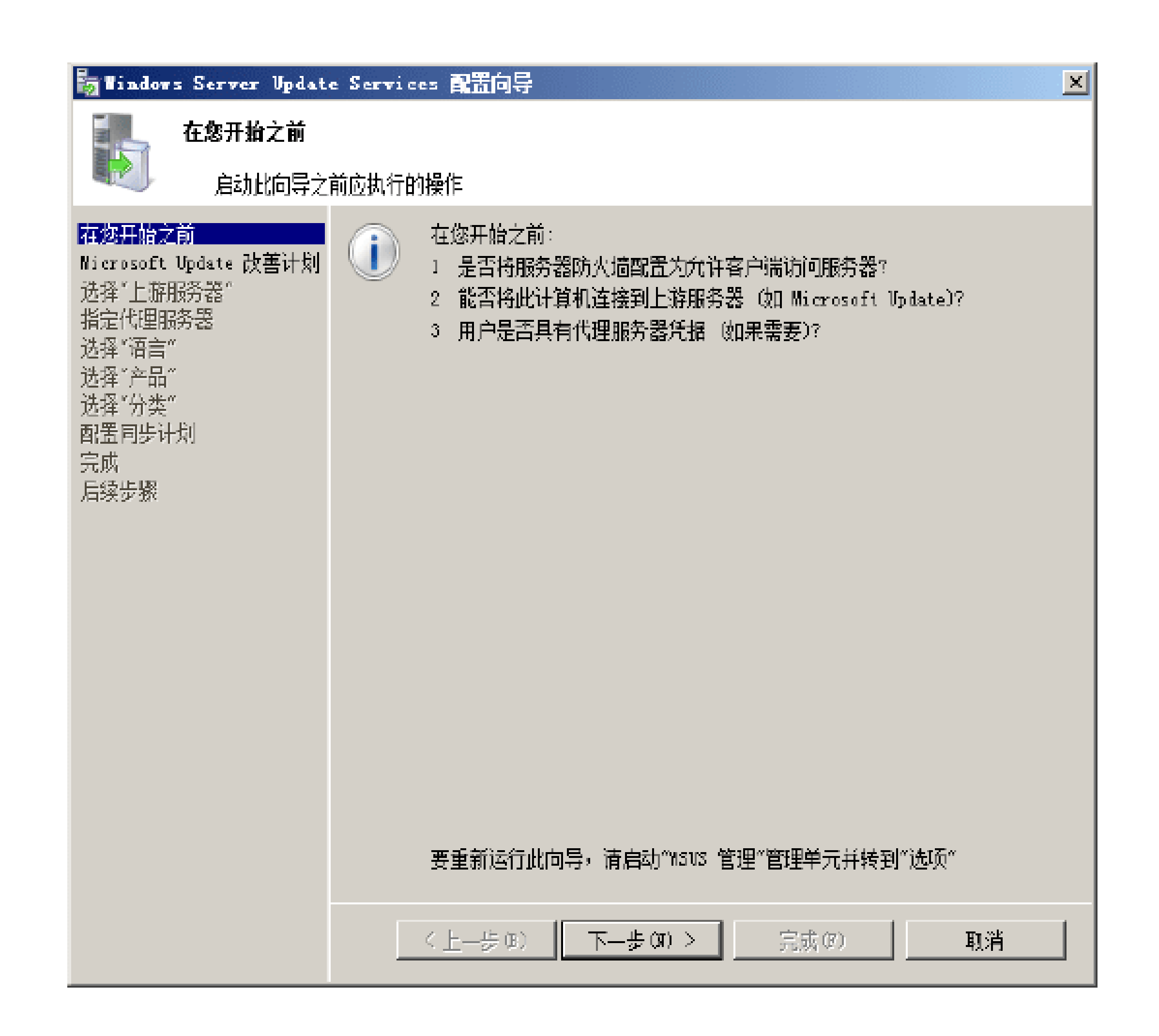


图 3.9　“Windows Server Update Services 配置向导”对话框

（5）配置 WSUS 服务器常规选项

按照默认设置安装 WSUS 服务器后，必须经过详细配置，才可以开始工作，包括设置接入 Internet 方式、获取更新方式、支持产品分类、同步方式及时间等。

01 在“Windows Server Update Services 配置向导”的“在您开始之前”页面中，依次单击“下一步”按钮，根据需要设置上游服务器类型、代理服务器等，如图 3.10 所示。在“选择‘上游服务器’”对话框中，系统默认选择“从 Microsoft Update 进行同步”单选按钮，即直接从微软服务器获取更新程序。如果网络中已经存在“上游 WSUS 服务器”，则可以选择“从其他 Windows Server Update Services 服务器进行同步”，并在“服务器名”文本框中，输入上游 WSUS 服务器的 IP 地址或计算机名，在“端口号”文本框中，输入上游 WSUS 服务器的端口号。

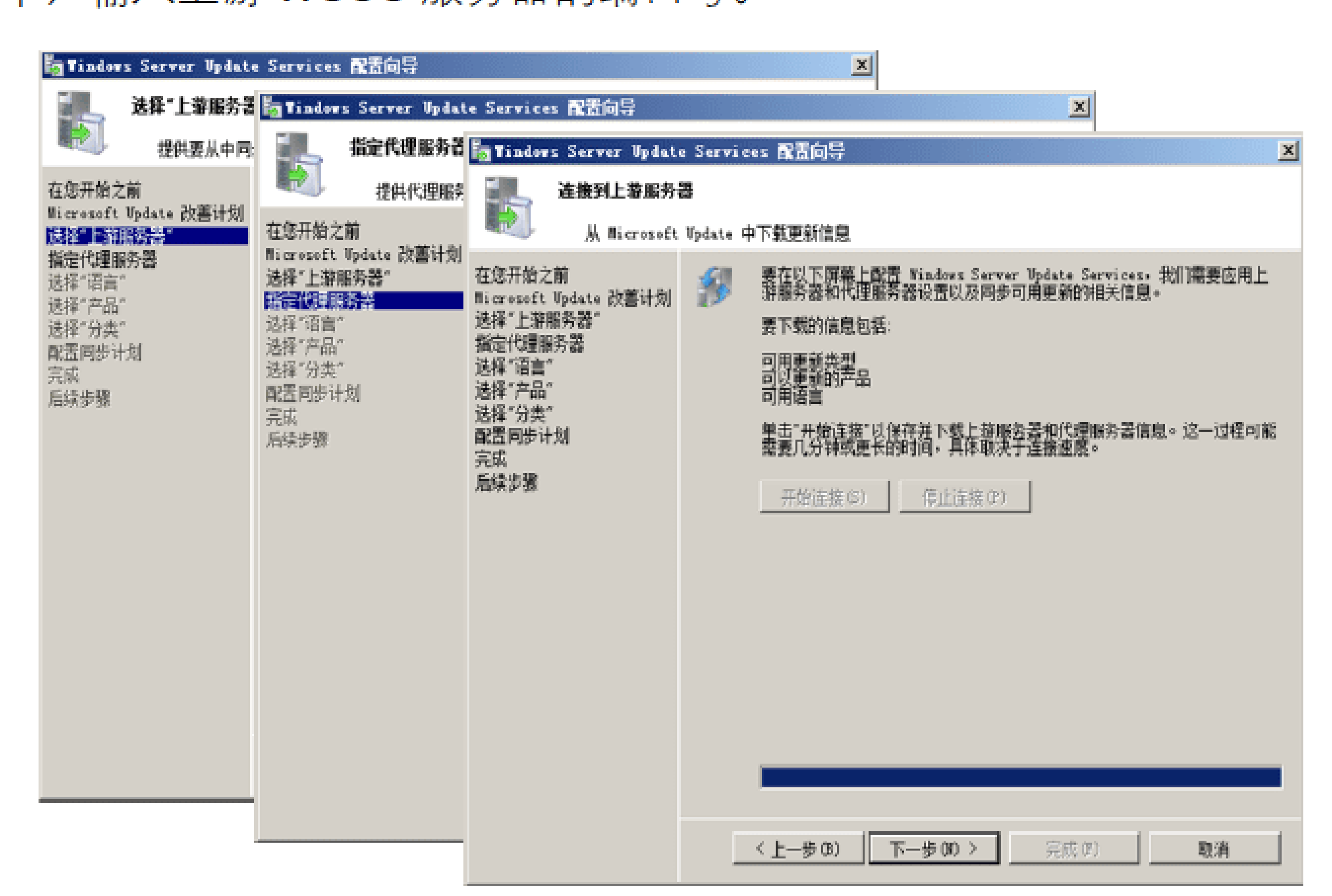


图 3.10　选择上游服务器并尝试连接

提示　选择本地网络的上游 WSUS 服务器时，如果使用的上游服务器使用了 SSL 通信方式，则此处也应选中“在同步更新信息时使用 SSL”复选框。需要注意的是，部署 SSL 会增加 WSUS 服务器 10%左右的工作负荷，并且这种传输加密机制仅能用于 WSUS 元数据通信，而并非是所有需要传输的更新文件。

02 连接完成后，依次单击“下一步”按钮，设置更新包语言种类、产品类型等，如图 3.11 所示。WSUS 支持的产品类型比较多，为了避免下载过多不必要的更新，建议用户严格选择适合自己的产品类型，更新语言包和种类的选择同样如此。根据网络需求的变化，管理员可以随时修改这些设置。

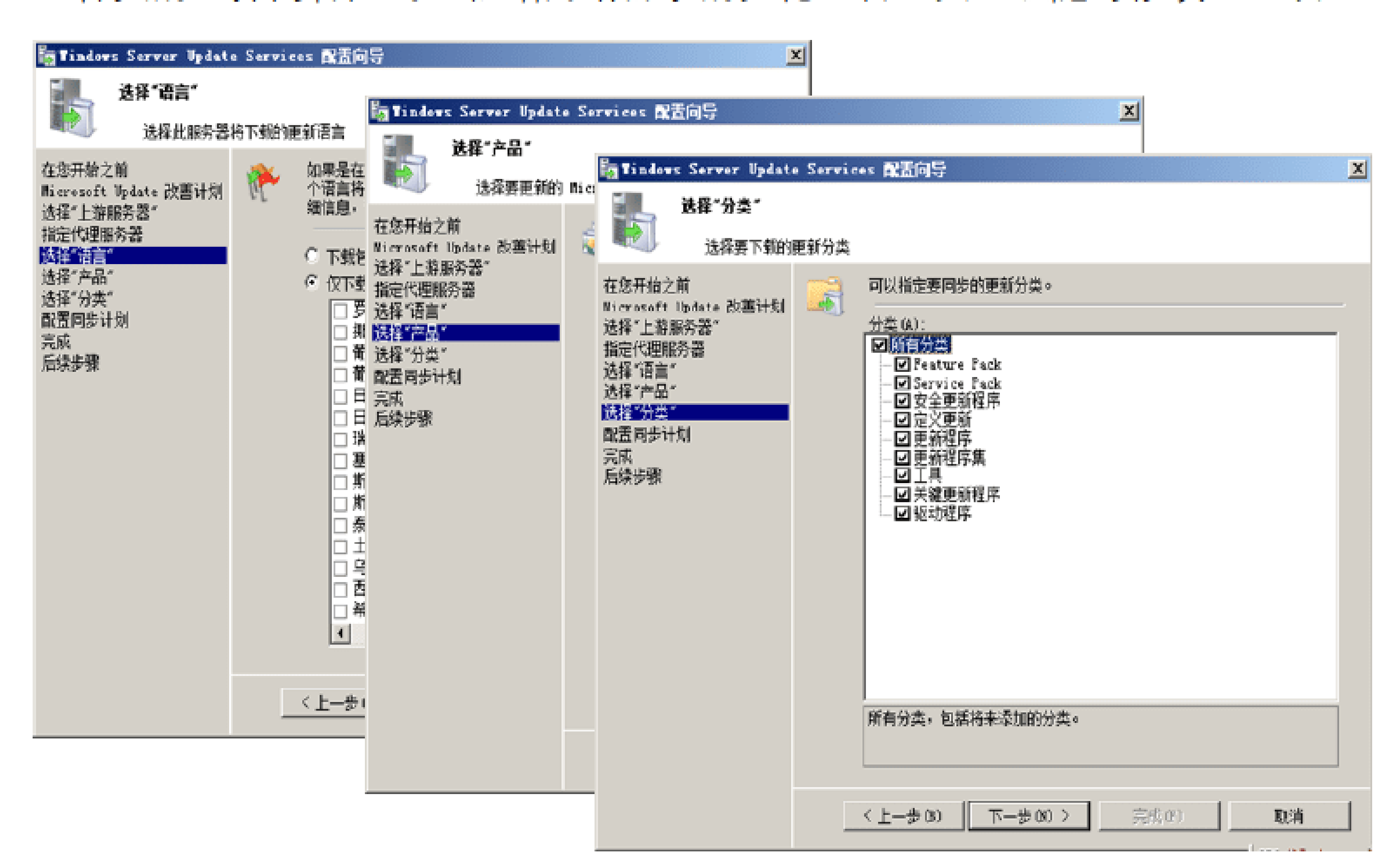


图 3.11 设置更新包语言、产品及分类



注意 如果当前 WSUS 服务器是从“上游”WSUS 服务器更新，将显示“下载上游服务器支持的所有语言的更新”或“仅下载这些语言的更新（上游服务器只支持标有星号的语言）”。

03 依次单击“下一步”按钮，设置同步计划并完成 WSUS 服务器的配置，如图 3.12 所示。在“设置同步计划”对话框中，建议选择“自动方式”，并将同步时间选择在网络空闲的时间段内，避免影响其他网络应用。配置向导完成后提示的后续步骤是可选的，管理员可以根据需要选择配置。

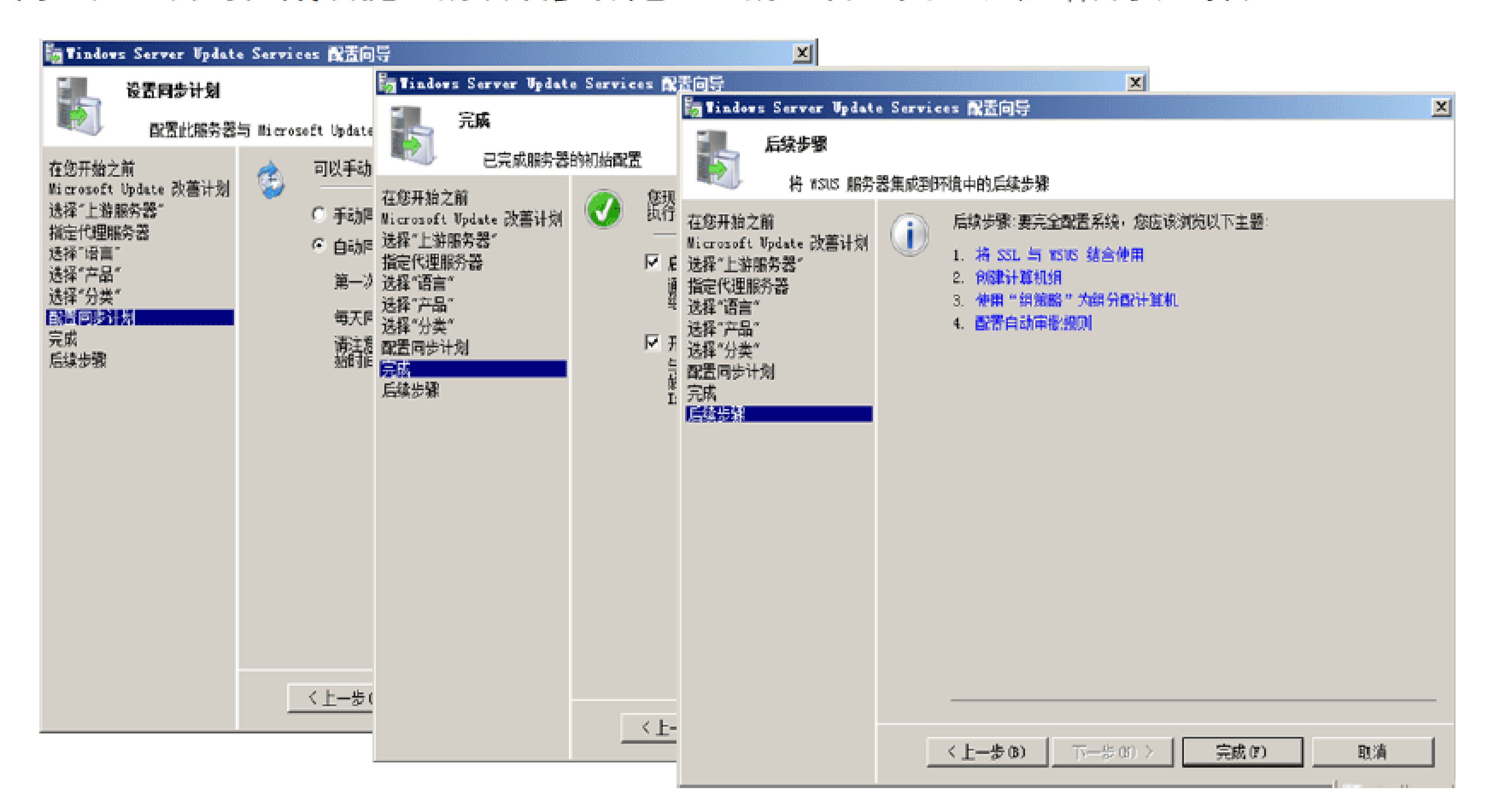


图 3.12 配置同步计划

04 单击“完成”按钮，完成配置向导即可。

（6）计算机及分组管理

WSUS 对客户端的管理都是通过分组的方式进行的，分组标准非常灵活，可以根据所需



更新类型的不同划分，也可以根据所属部门的不同进行划分，也可删除多余分组。默认情况下，所有 WSUS 客户端都将存储在“未分配的计算机”分组中，管理员可以根据需要将其迁移或复制到其他分组。

如果需要删除计算机分组，可以在“Update Services”窗口中，右击分组名称，选择快捷菜单中的“删除”，打开如图 3.13 所示“删除计算机组”对话框。这里包括 3 个单选按钮：

- 从此组中删除计算机：只删除当前分组中的计算机，而不会影响到计算机在其他分组中的存在和应用；
- 将计算机移到此组的父组中：将组中的计算机移动到其父组中，由于当前组的父组是“所有计算机”，默认已经存在该计算机，所以不可操作；
- 从此 WSUS 服务器中删除计算机：彻底删除本组的计算机，如果其他分组中也有该计算机则一同删除。

正确配置 WSUS 客户端后，服务器将自动发现这些客户端，显示在“未分配的计算机”分组中，如图 3.14 所示。如果没有立即显示，可以尝试刷新一下服务器，或者在“状态”下拉列表中选择适当的状态，如“任何”等。

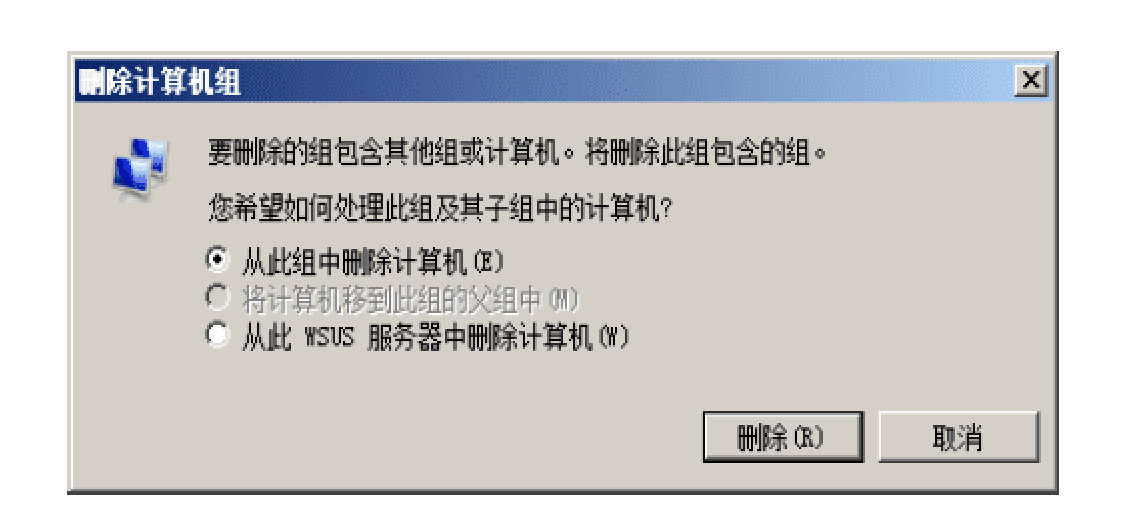


图 3.13　“删除计算机分组”对话框

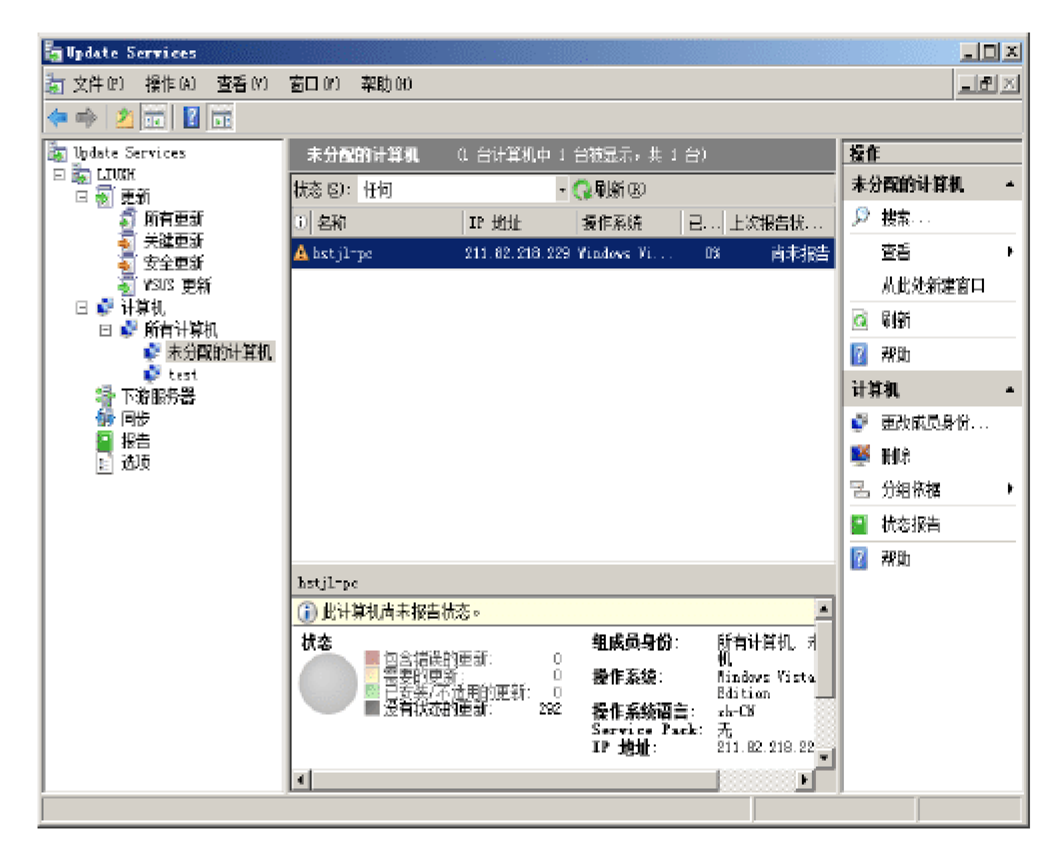
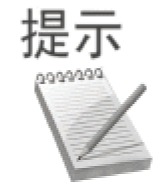


图 3.14　发现的客户端计算机

如果接受管理的 WSUS 客户端数量较多，则可以通过“搜索”功能快速查找指定的计算机。

提示



如果使用客户端计算机上的组策略或注册表设置管理客户端，则无法完成此设置。

3. 同步和管理更新

（1）执行同步

“同步”就是当前 WSUS 服务器从 Microsoft Update 站点或其上游 WSUS 服务器获取所需更新的过程，用户可以通过手动同步和自动同步两种方式来实现。如果采用每天定时同步，则根据自己企业的外部网络访问情况来决定何时进行同步，应计划为外部网络访问活动较少的时段，例如凌晨。如果网络带宽资源紧张，则可以保持默认的手动同步方式。

执行 WSUS 服务器同步是一项非常关键的操作，如果制定了同步计划，只需打开计算机系统

就会自动完成，当然也可以采取手动的方式。右击“同步”并选择快捷菜单中的“立即同步”，或者在“操作”选项框中单击“立即同步”链接，即可开始同步，如图3.15所示。需要注意的是，在同步过程中将不会显示同步开始的时间、同步类型、结果等信息，但是可以在下面的信息提示框中查看到当前的同步进度。同步过程中如需停止，则单击“停止同步”链接即可。

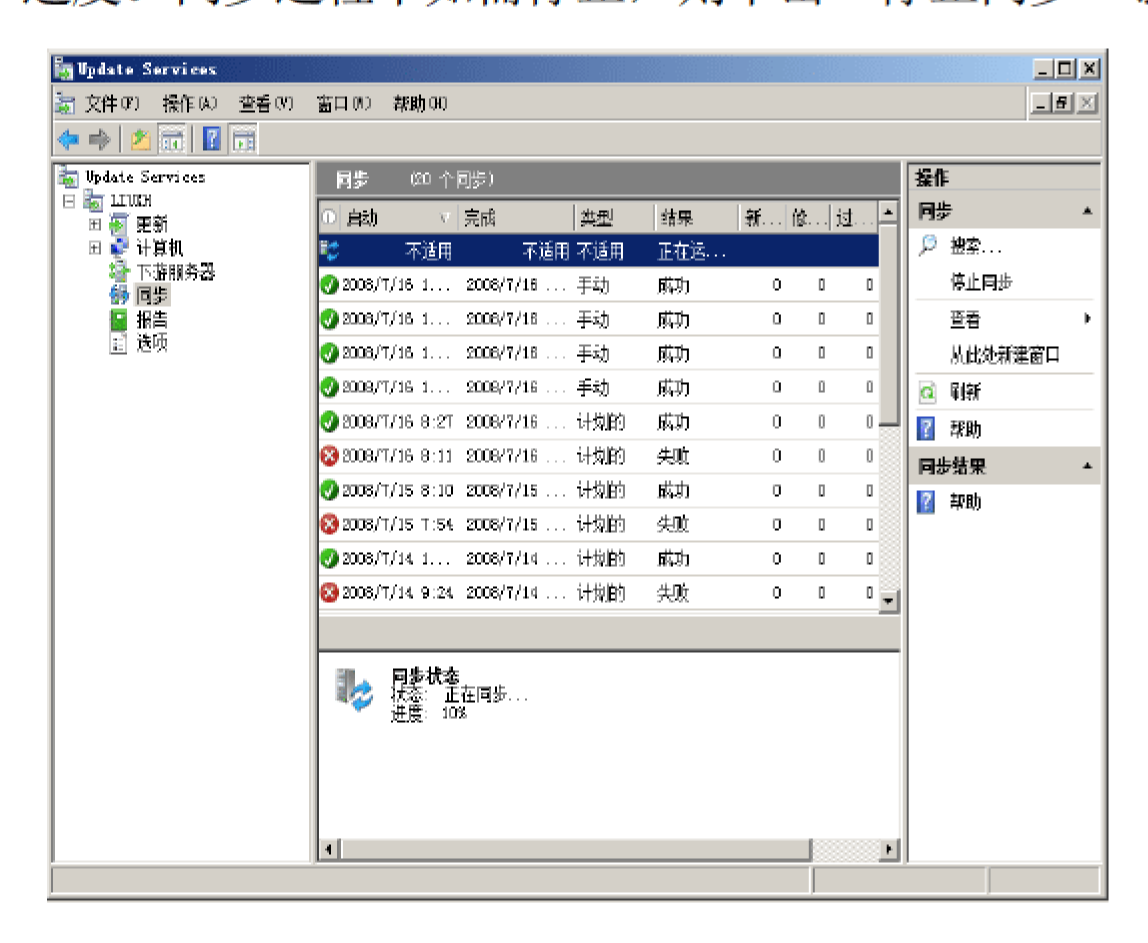


图 3.15　正在同步

（2）查看和管理更新程序

在“Update Services”窗口中，展开“同步”分支，将自动显示最近完成的几次同步信息，如图 3.16 所示，包括同步启动时间、完成时间、类型、结果等。在更新结果列表中单击某一次同步记录时，即可在下面信息窗口中显示此次同步的详细情况。

WSUS 服务器的同步报告信息当然不会像这里显示的这样简单，右击同步记录并选择快捷菜单中的“同步报告”即可查看所选同步的详细信息，如图 3.17 所示。其中包括同步摘要信息以及此次同步中新的更新程序、修改更新和过期更新等。

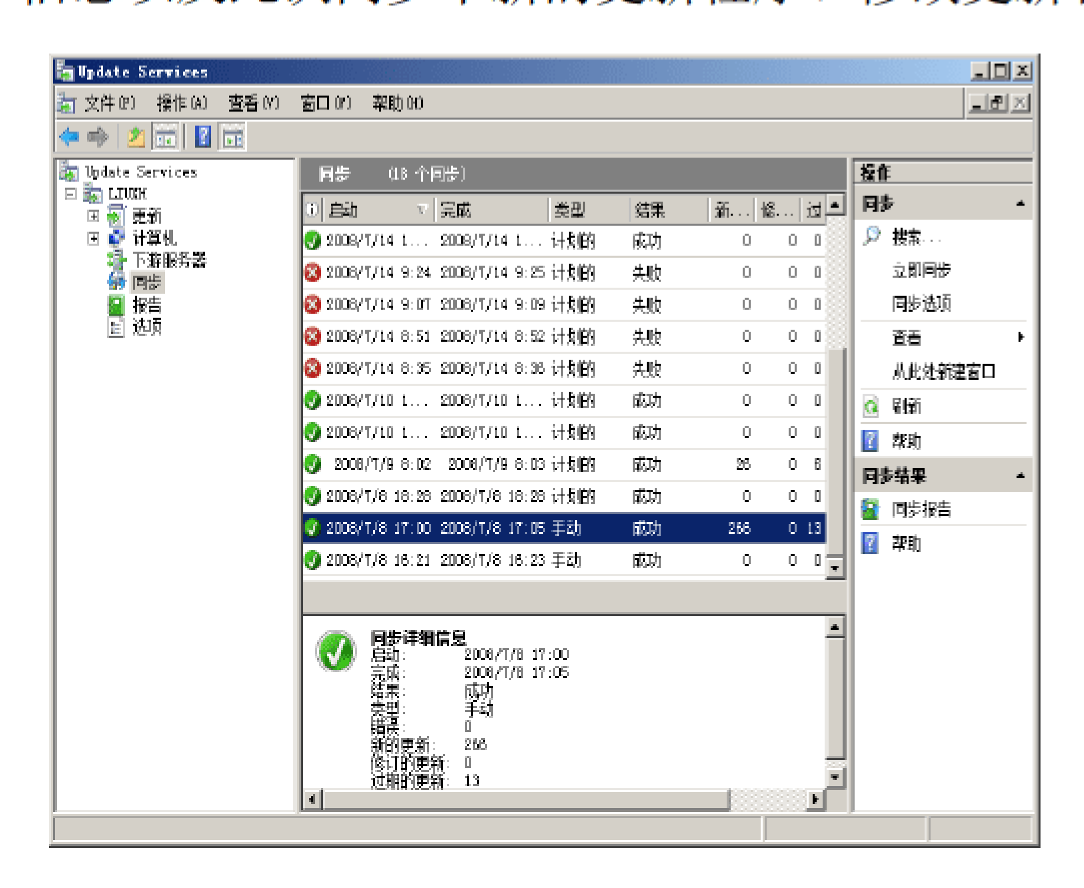


图 3.16　查看同步信息

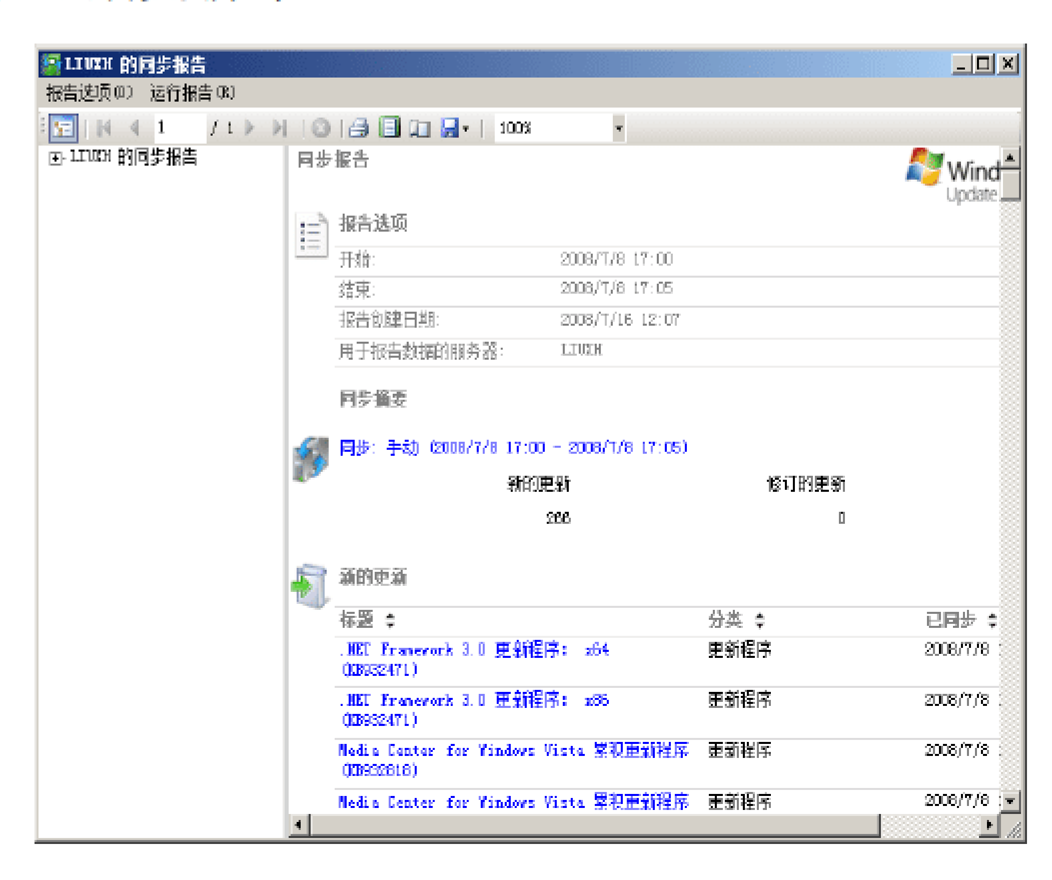


图 3.17　“同步报告”窗口

除此之外，管理员还可以查看此次同步中某个更新的详细信息，单击希望查看的更新，打开如图 3.18 所示“更新报告”窗口，其中包括该更新的描述信息、所属类型、发布日期等常用信息。这恰恰是判断一个更新是否对客户端有用的有效途径。例如在通过 Windows 自动更新为自己的计算机安装已下载的更新时，往往要先看清它的描述信息，可以弥补哪些漏洞，安

装之后会产生什么影响等。



图 3.18　“更新报告”窗口

4. 为客户端审批更新

（1）创建审批规则

在 WSUS 主窗口的“选项”列表中，单击“自动审批”链接，显示如图 3.19 所示“自动审批”对话框。在这里即可对 WSUS 服务器的自动批准规则进行设置，如添加某项新规则、删除或编辑现有规则等。默认情况下，WSUS 服务器是不运行任何自动审批规则的，即完全由管理员手动审批完成。通过启用自动审批功能，可以将特定的分类和产品类型的更新，审批到指定的客户端，这样可以大大减轻管理员的工作负担，但仅限于可靠性较高的更新。为避免安装更新之后可能导致的各种麻烦，建议审批之前进行严格测试，确认无误后再审批到客户端。

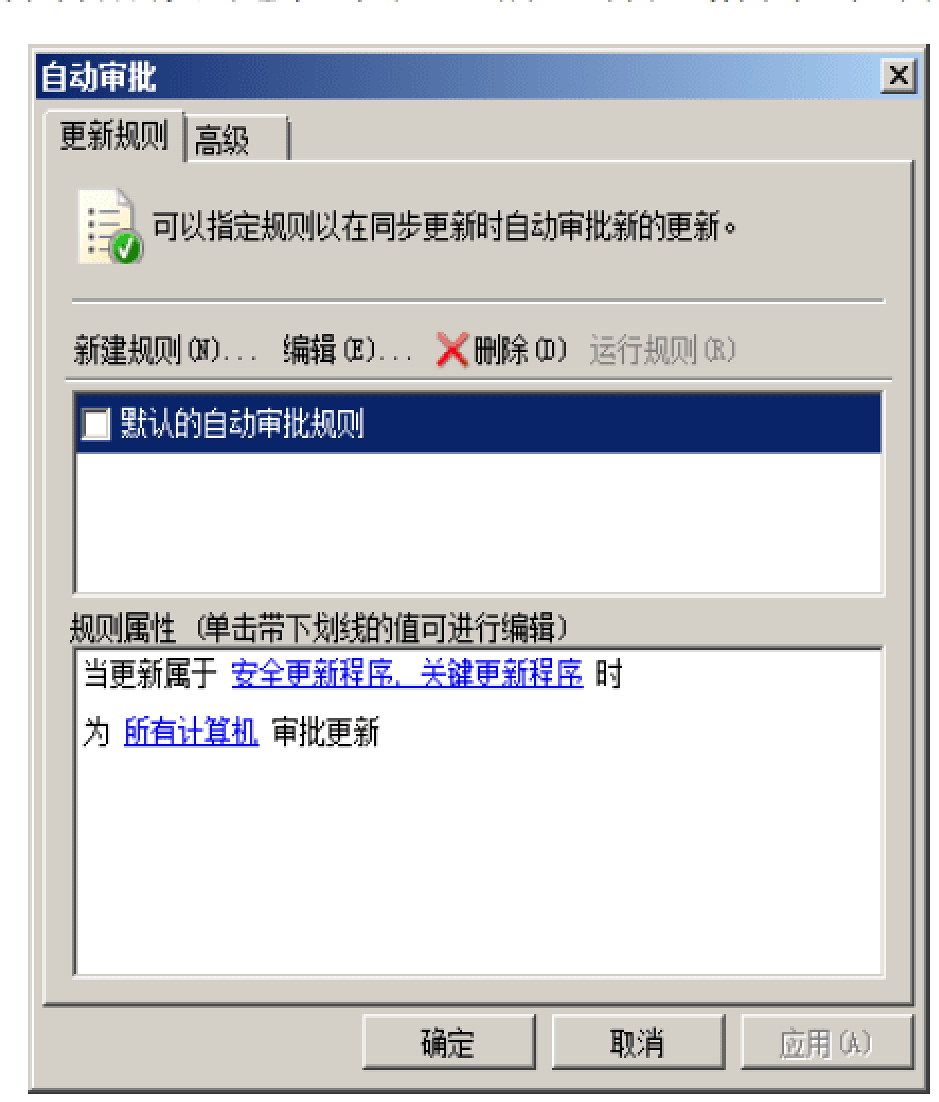


图 3.19　“自动审批”对话框

01 单击“新建规则”按钮，显示如图 3.20 所示“添加规则”对话框。首先在“步骤 1：选择属性”选项框中，选择希望用于批准特定分类更新还是审批用于特定产品的更新；选中某一项前面的复选框的同时，在“步骤 2：编辑属性”选项框中也会自动增加针对该项的详细设置；在“步骤 3：指定名称”文本框中输入新规则的名称。

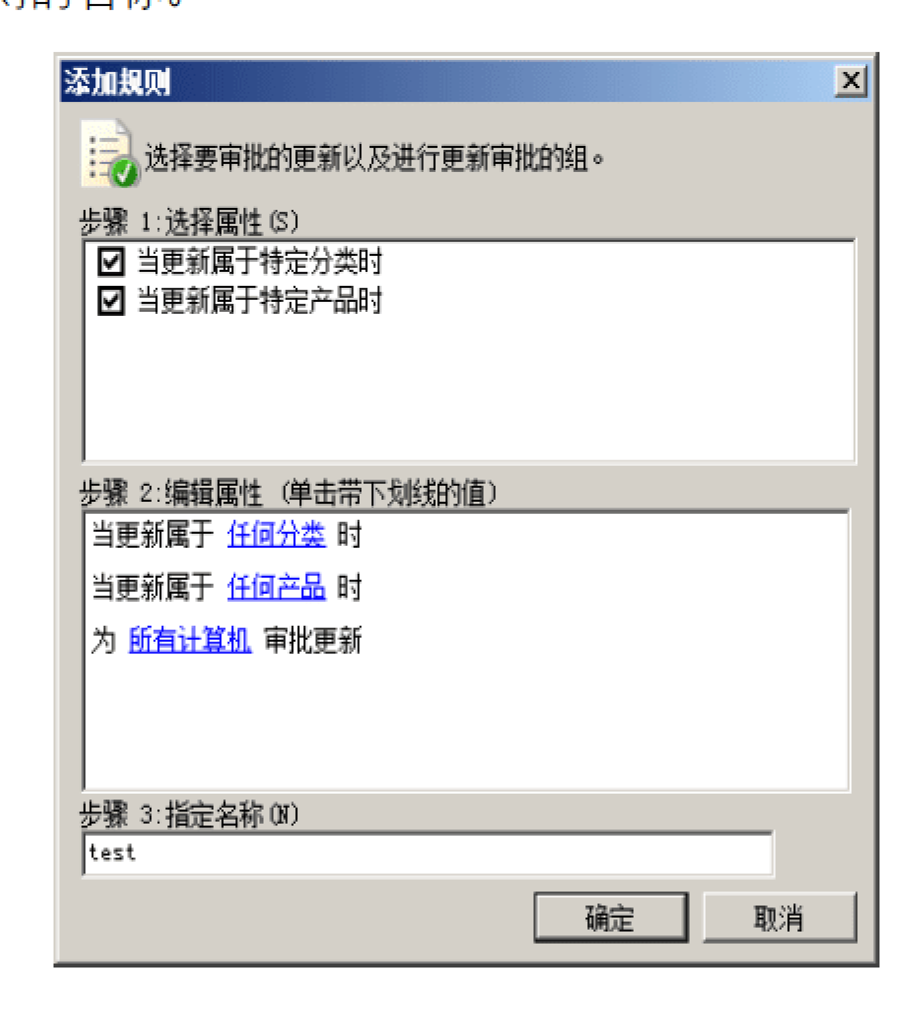


图 3.20 “添加规则”对话框

02 在“步骤 2：编辑属性”编辑分类选项框中，还可以对选定的分类进行详细编辑。例如单击“任何分类”超级链接，打开如图 3.21 所示“选择‘更新分类’”对话框。默认状态下，列表中的所有产品都是被选中的，有些产品类型并不是需要的，只需在这里将其取消即可。单击“确定”按钮保存设置并返回“自动审批”对话框。

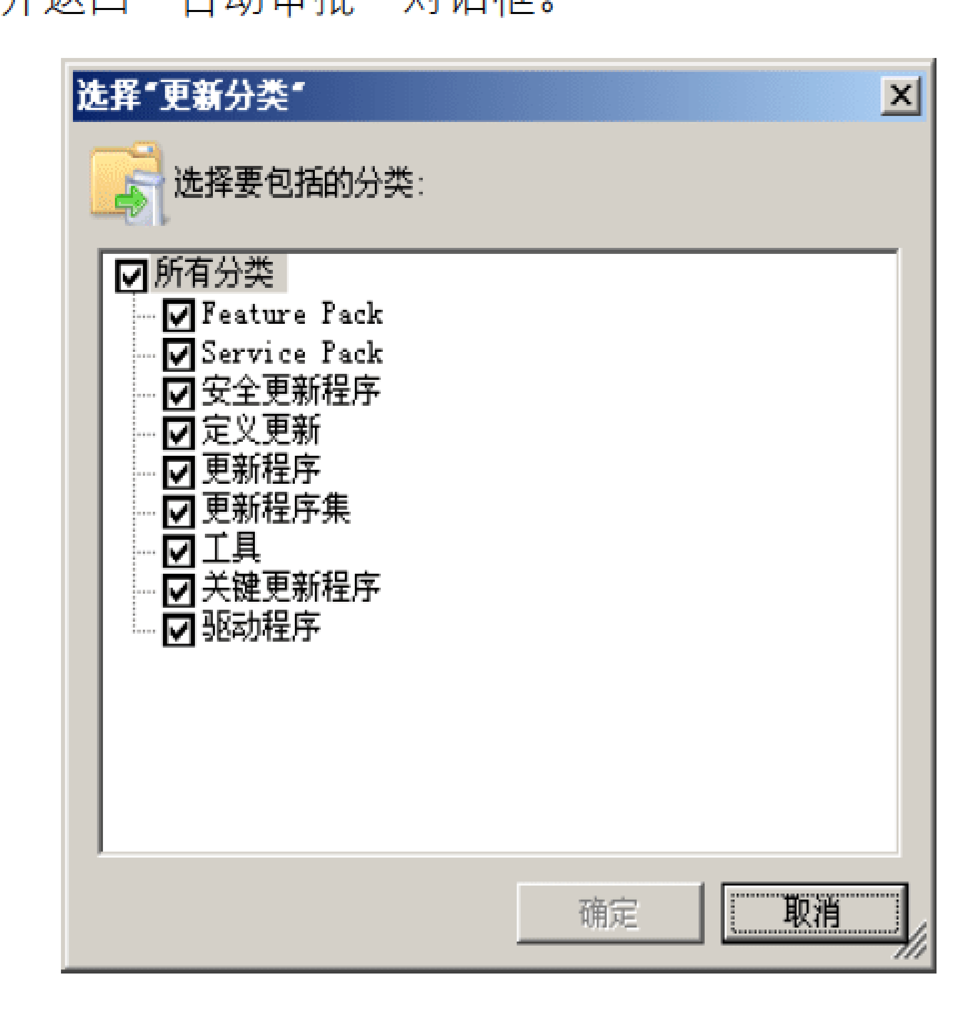


图 3.21 “选择‘更新分类’”对话框

03 选中成功创建的审批规则后，单击“运行规则”按钮，打开如图 3.22 所示“运行规则”提示框，提示用户启用规则之前需要先进行保存，是否要继续。



图 3.22 “运行规则”提示框

04 单击“是”按钮即可开始运行，此时 WSUS 服务器会根据所选自动批准规则中的限制和过滤条件，筛选可用的更新安装程序，可能需要等待一段时间。成功完成后，显示如图 3.23 所示结果，提示被自动批准的更新的数量。



图 3.23 “正在运行规则”提示框

05 单击“关闭”按钮将保存设置即可。

在“自动审批”对话框中，单击“高级”切换至如图 3.24 所示“高级”选项卡，默认情况下，系统自动审批 WSUS 更新和更新修订，并自动拒绝过期的更新，用户也可以根据实际需要暂时将其取消。

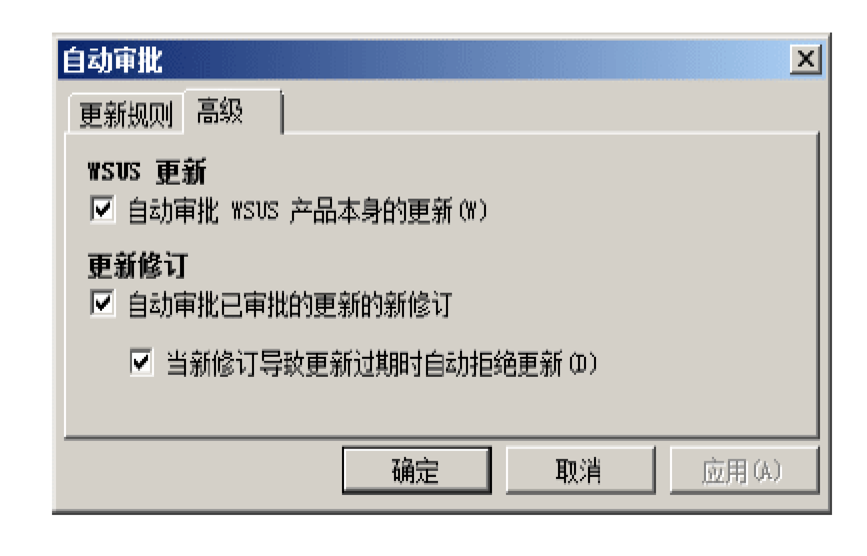


图 3.24 “高级”选项卡

（2）审批更新

审批更新是指管理员在 WSUS 服务器上配置，允许或拒绝分发到客户端的更新程序。管理员可以根据需要为所有计算机或特定计算机组审批更新，并设置 WSUS 安装更新的最后期限。对于不适用于指定客户端的更新，也可以选择拒绝审批或删除。

01 在更新程序详细信息窗口中（以“所有更新”为例），右击需要审批的更新并选择快捷菜单中的“审批”，打开如图 3.25 所示“审批更新”对话框。

02 单击需要安装该更新的计算机分组，选择下拉菜单中的“已审批进行安装”，即可将更新审批到该组中的所有计算机，如图 3.26 所示。默认情况下，分组将自动继承其父分组的审批设置。

- 已审批进行安装。客户端将直接安装该更新；
- 已审批进行删除。如果该更新是允许删除的，则客户端将自动删除该更新程序；
- 未审批。客户端既不安装也不删除更新。

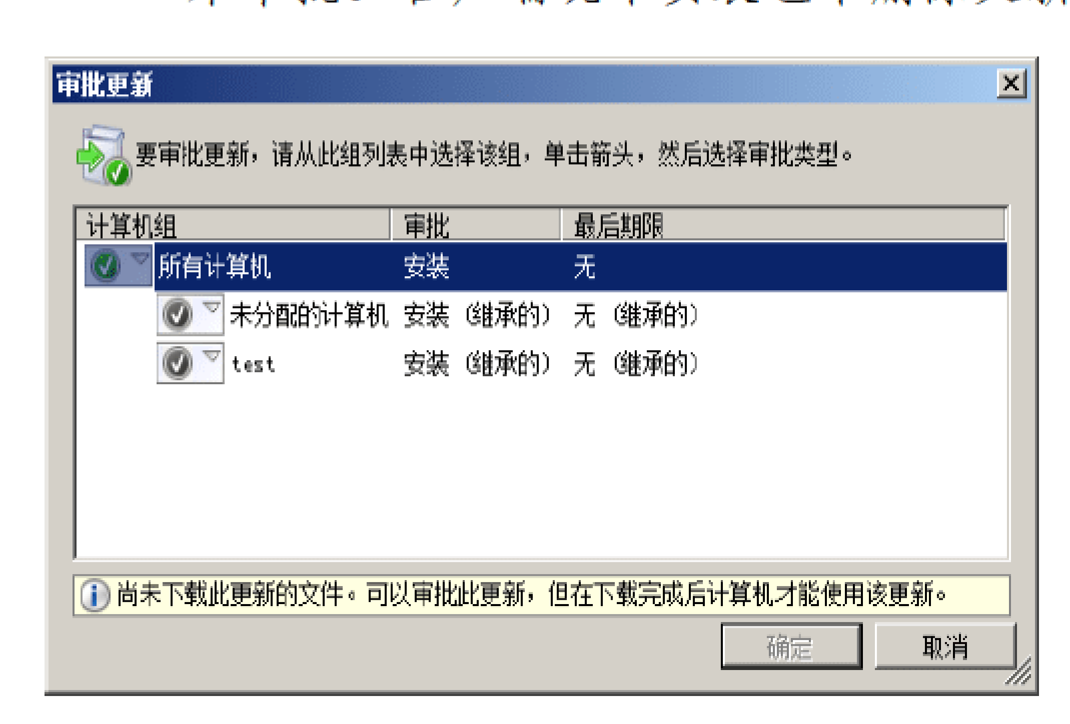


图 3.25　“审批更新”对话框

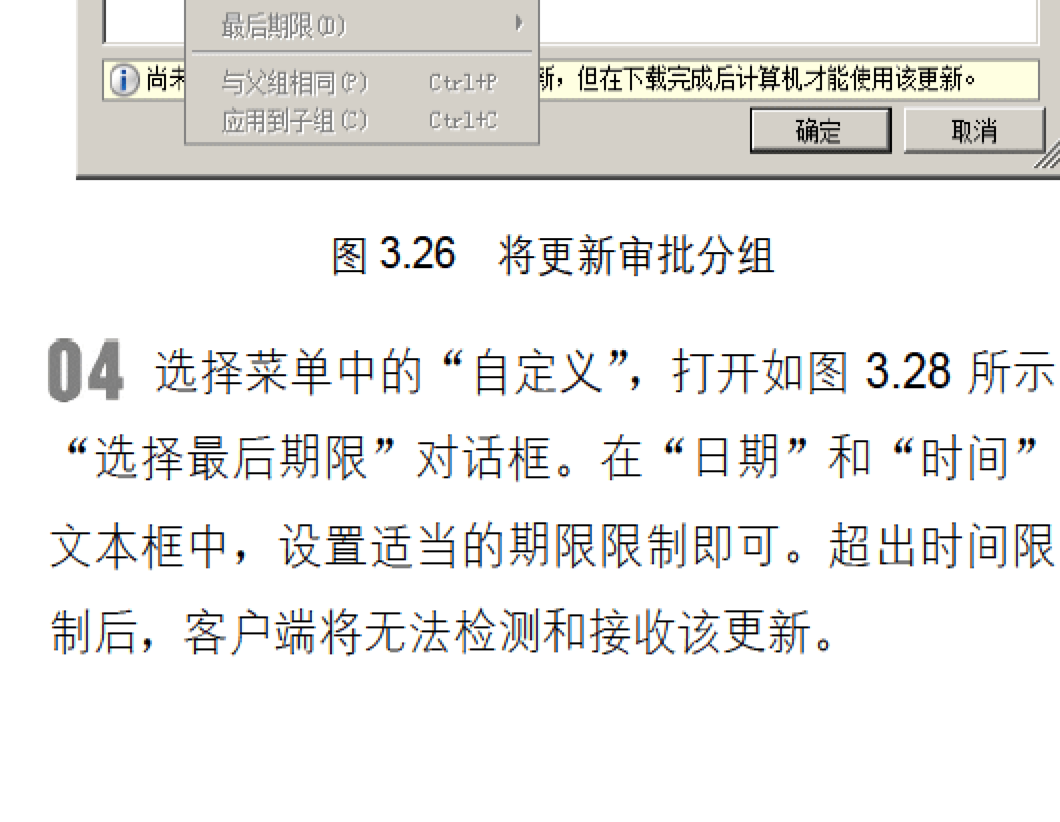


图 3.26　将更新审批分组

03 审批安装之后分组前的图标将显示为绿色，继续单击该图标并选择菜单中的“最后期限”，选择希望设置的期限即可，如图 3.27 所示。默认为无最后期限，即自 WSUS 服务器发布更新之日起，客户端可以在任何时间接收更新。

04 选择菜单中的“自定义”，打开如图 3.28 所示“选择最后期限”对话框。在“日期”和“时间”文本框中，设置适当的期限限制即可。超出时间限制后，客户端将无法检测和接收该更新。

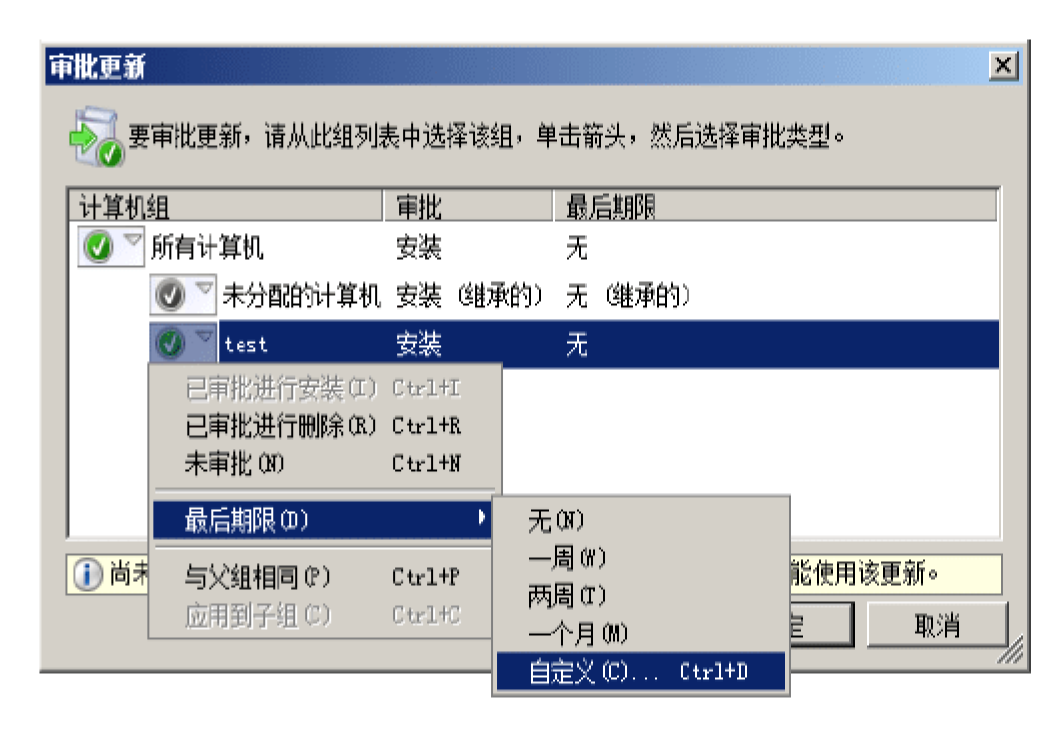


图 3.27　设置最后期限

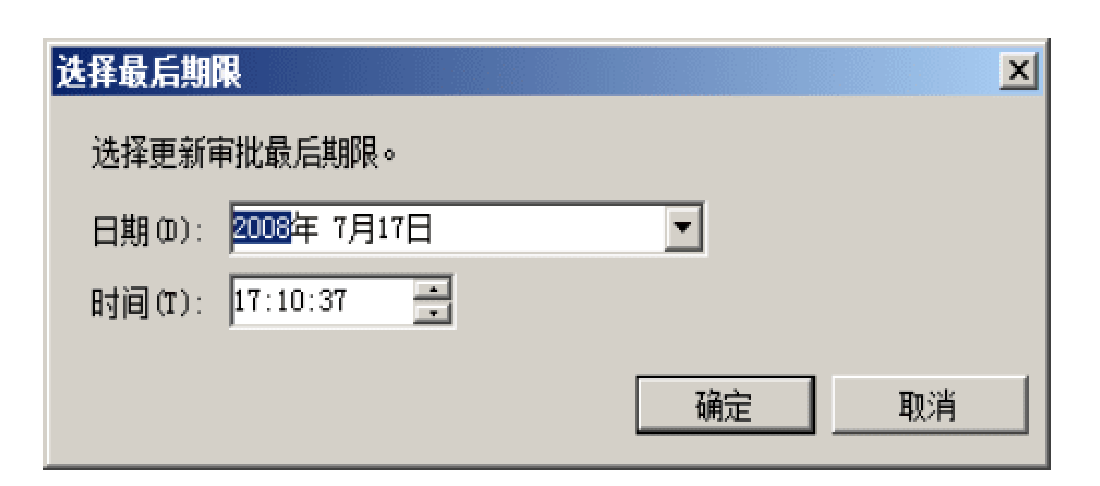


图 3.28　“选择最后期限”对话框

05 连续单击“确定”按钮，显示如图 3.29 所示“审批进度”对话框，根据审批更新数量的不同，所需时间也会有所不同。如果出现错误，审批结果中会显示为“失败”。

06 单击“关闭”按钮，关闭“审批进度”对话框，返回“Update Services”窗口。

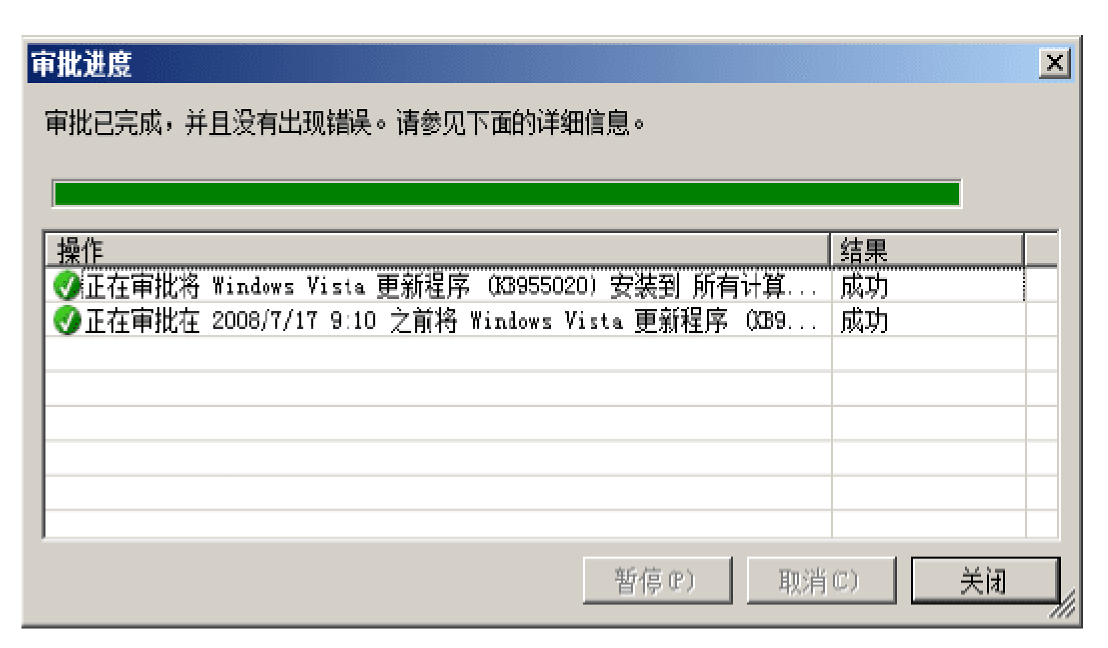


图 3.29　“审批进度”对话框

（3）拒绝更新

如果某个更新不再适用于当前网络，则可以在 WSUS 服务器的更新管理窗口中将其拒绝。在拒绝更新时，默认情况下，“更新”窗口中不再显示，并且无法对其进行审批，只能在“更新”窗口中查看被拒绝的更新。

01 右击想要拒绝的更新，并选择快捷菜单中的“拒绝”选项，显示如图 3.30 所示“拒绝更新”对话框。

02 单击“是”按钮，确认拒绝即可。等待一段时间或单击工具栏中的“刷新”按钮，即可发现该更新程序的“审批”状态已变为“已拒绝”，如图 3.31 所示。

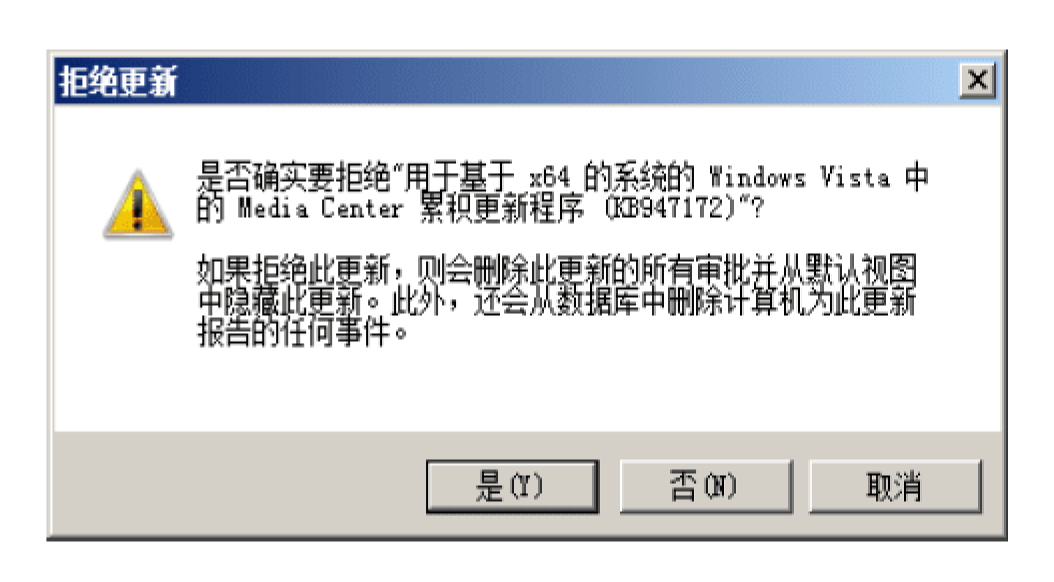


图 3.30　“拒绝更新”对话框

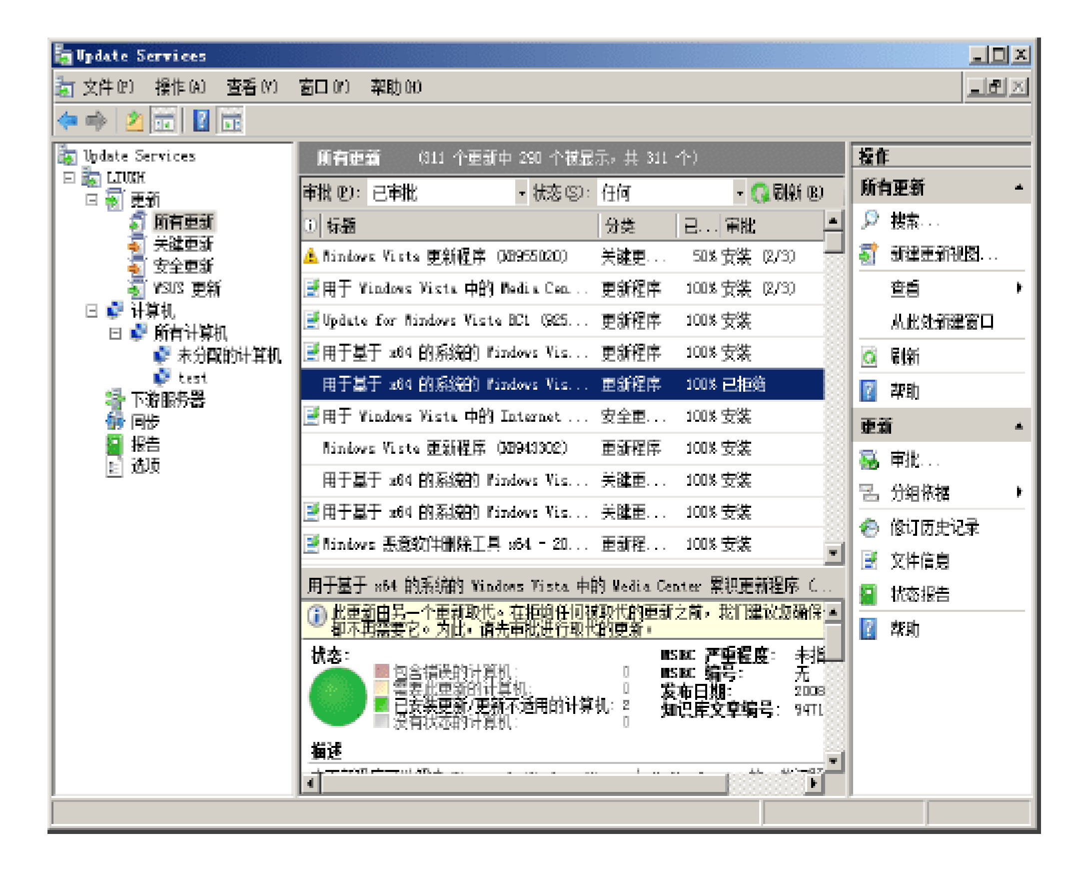


图 3.31　被拒绝的更新

5. 配置 WSUS 客户端

凡是具备自动更新功能的 Windows 操作系统，都可以配置为 WSUS 客户端。根据客户端计算机所在网络环境的不同，可以采取不同的配置方法。在域环境中，可以使用组策略对象（GPO）完成；在工作组环境中，可以使用本地组策略对象或者直接修改注册表完成。需要注意的是，将计算机配置为 WSUS 客户端后，客户端计算机“控制面板”中的自动更新就会失效。



（1）通过组策略编辑器配置

如果通过组策略为 Active Directory 网络中的计算机指定 WSUS 升级服务器的地址，需要在包括网络中所有计算机的“组织单元”或其上一级“组织单元”中配置组策略，或者将需要更新的计算机“移动”到一个新创建的“组织单元”中，然后再对该组中的所有计算机进行操作。

01 新建一个用于保存所有 WSUS 客户端计算机的组织单位，当然也可以使用 Active Directory 默认提供的组织单位。

02 使用新建计算机的方法将客户端计算机添加到指定的组织单位中，也可以从其他组织单位中直接拖拽。

03 依次选择“开始”→“管理工具”→“组策略管理”选项，打开“组策略管理”窗口，依次展开“林”→“域”→“company.com”选项→“test（新建的组织单位）”选项。

04 右击“test”并选择快捷菜单中的“在这个域中创建 GPO 并在此处链接”选项，打开如图 3.32 所示“新建 GPO”对话框，在“名称”文本框中，输入便于识别的名称。

05 右击新建的 GPO 并选择快捷菜单中的“编辑”选项，打开如图 3.33 所示“组策略管理编辑器”窗口。依次展开“计算机配置”→“策略”→“管理模板”→“Windows 组件”→“Windows Update”分支，即可看到所有的设置选项，默认都是未被配置的。

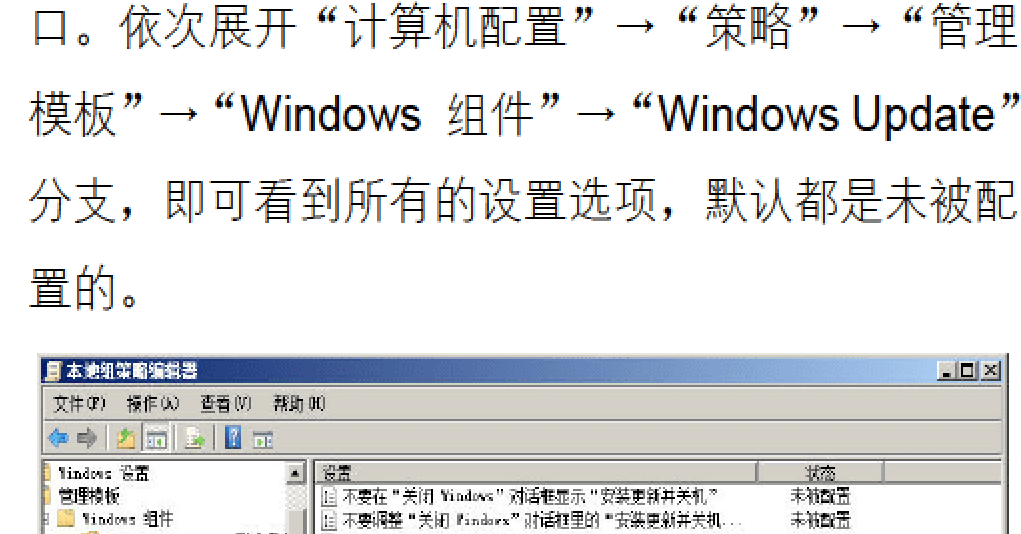




图 3.32　“新建 GPO”对话框

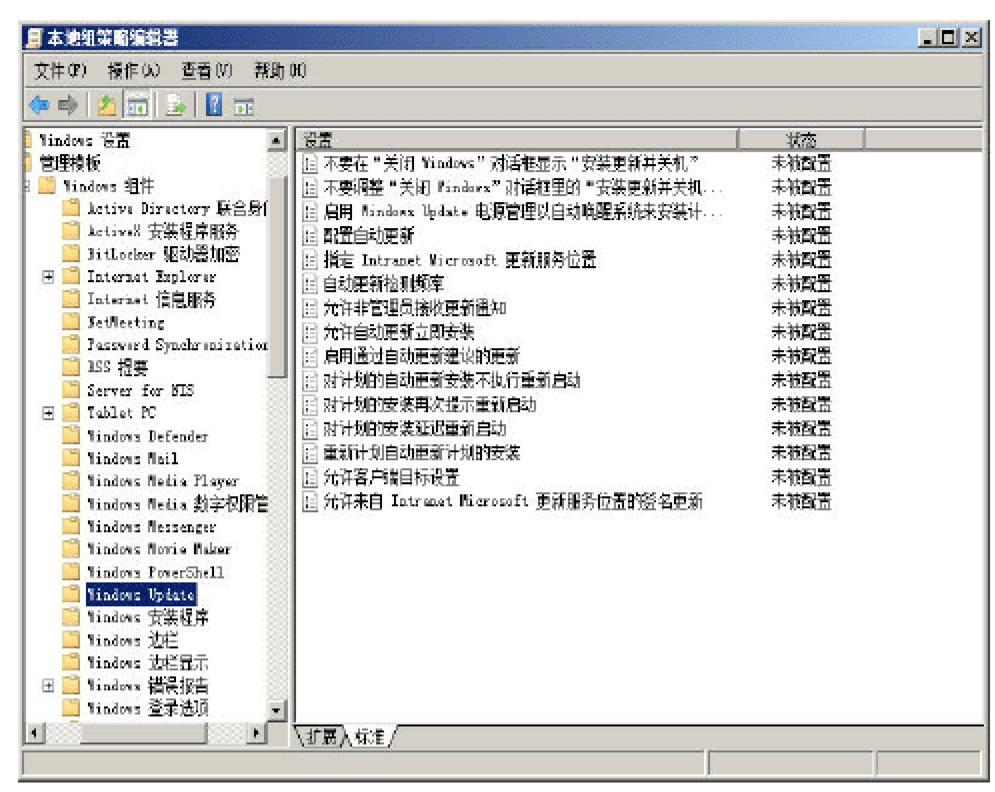


图 3.33　对应策略所在目录

06 双击“配置自动更新”选项，打开如图 3.34 所示“配置自动更新 属性”对话框，先选中“已启用”单选按钮激活下面的选项，然后在“配置自动更新”右侧的下拉列表中选择对应的自动更新类型，共有 2~5 四种类型，当选择第 4 种类型“自动下载并计划安装”，即自动下载更新并计划安装时还要继续设置“计划安装日期”和“计划安装时间”选项，指定执行安装的时间和日期。设置完成后单击“应用”和“确定”按钮保存设置。

07 双击“指定 Intranet Microsoft 更新服务位置”策略，显示如图 3.35 所示“指定 Internet Microsoft 更新服务位置 属性”对话框。选中“已启用”单选按钮，然后在“设置检测更新的 Intranet 更新服务”文本框中，指定局域网中的 WSUS 服务器地址，在“设置 Intranet 统计服务器”文本框中，指定用于获取客户端状态信息的服务器地址，本例中使用的是一台服务器。如果网络中的 WSUS 服务器和统计报表服务器（只用于获取客户端的状态和需求信息）分别是不同的服务器，则此处指定时应十分注意。

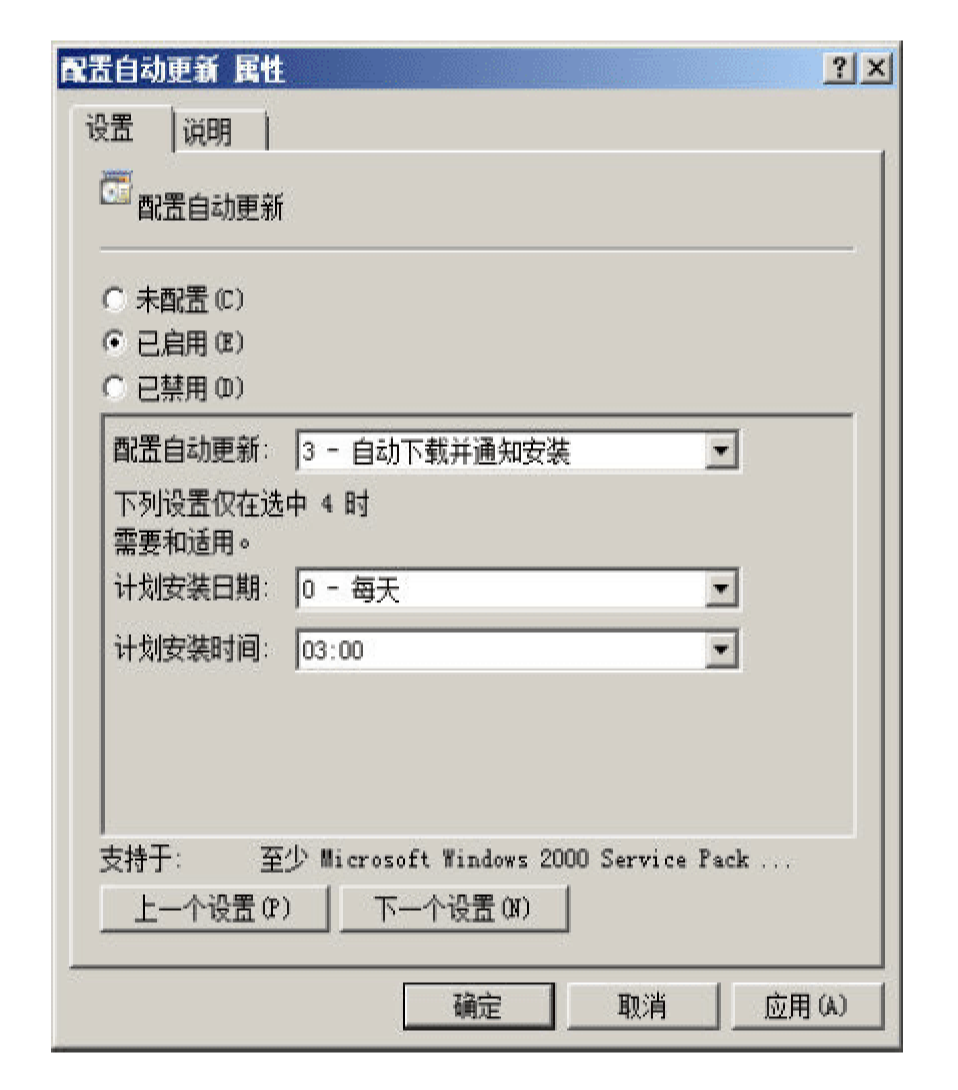


图 3.34　启用自动更新功能

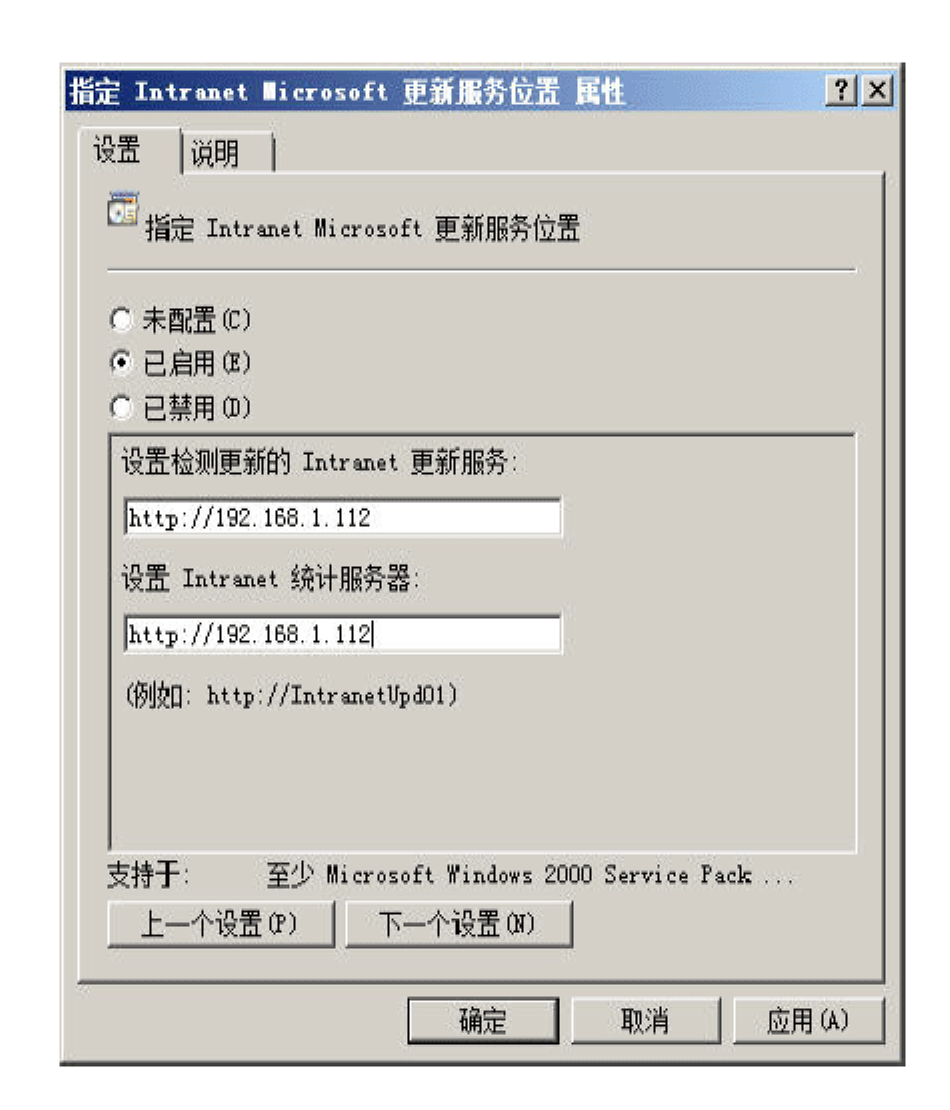


图 3.35　“指定 Internet Microsoft 更新服务位置 属性”对话框

注意

设置这两条策略的顺序千万不可颠倒，否则将不会生效，即必须先启用“配置自动更新”，然后才可以设置 WSUS 服务器地址。

08 保存组策略编辑结果即可。其他组策略现象用户也可以根据需要进行修改。由于组策略的刷新和应用需要一定的时间，所以保存编辑结果后即使客户端重新登录域控制器也可能无法立即联系到 WSUS 服务器。而默认情况下，每隔 90min 计算机组策略便会在后台刷新一次，刷新的时间可能随机偏移 0~30min，客户端计算机要在域控制器刷新组策略 20min 后才可以应用到组策略。如果想要以更快的速度刷新组策略，可以在服务器端设置组策略后，通过运行 gpupdate 命令让设置即时生效，并在客户端计算机通过运行 gpupdate/force 命令立刻生效。如果计算机不是 Active Directory 的成员，可以通过输入 wuauclt.exe /detectnow 来消除 20min 的延时。

（2）通过本地策略配置

通过组策略或本地策略编辑器配置 WSUS 客户端，是最常用的方法之一。对于域环境中的计算机，用户可以在域控制器上创建应用于需要配置客户端的组策略，并进行相应编辑；而工作组中的计算机则可以通过修改本地策略使其成为 WSUS 客户端。此处，以工作组环境中的 Windows Vista 客户端为例加以介绍。

01 以管理员帐户登陆计算机，依次单击“开始”→“所有程序”→“附件”→“运行”，打开如图 3.36 所示“运行”对话框，在“打开”文本框中输入“gpedit.msc”，并单击“确定”按钮，打开“策略对象编辑器”窗口。除此之外，也可以在“开始”菜单中的“开始搜索”文本框中，输入“gpedit.msc”并回车打开“策略对象编辑器”窗口。

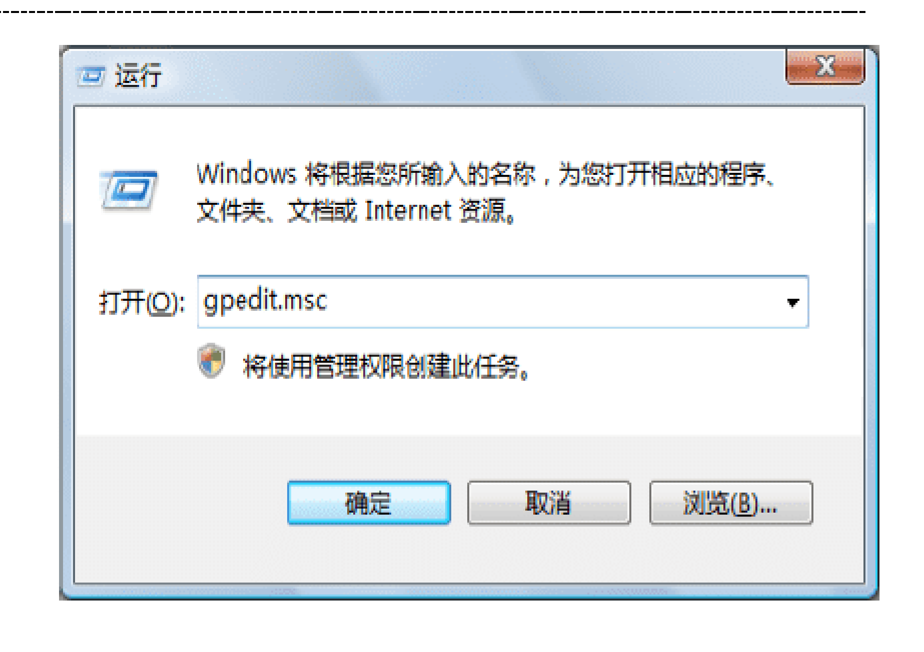


图 3.36　“运行”对话框



02 在“组策略对象编辑器”窗口中，依次展开“计算机配置”→“管理模板”→“Windows 组件”→“Windows Update”选项，如图 3.37 所示。与配置域组策略完全相同，需要依次配置“配置自动更新”和“指定 Intranet Microsoft 更新服务位置属性”策略，配置过程此处不再赘述。

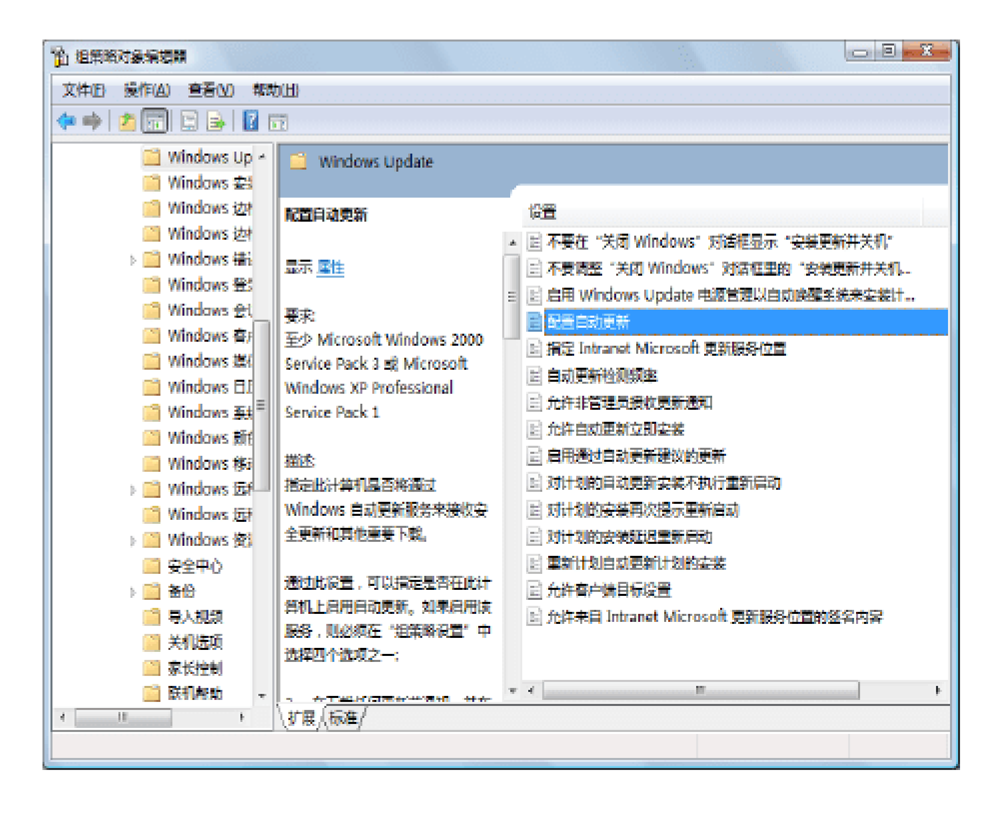


图 3.37　“组策略对象编辑器”窗口

03 配置完 WSUS 客户端后，在 Windows 目录下会生成 windowsupdate.log 文件，通过它可以看到此客户端是从何处升级的补丁以及升级了哪些补丁，如图 3.38 所示。

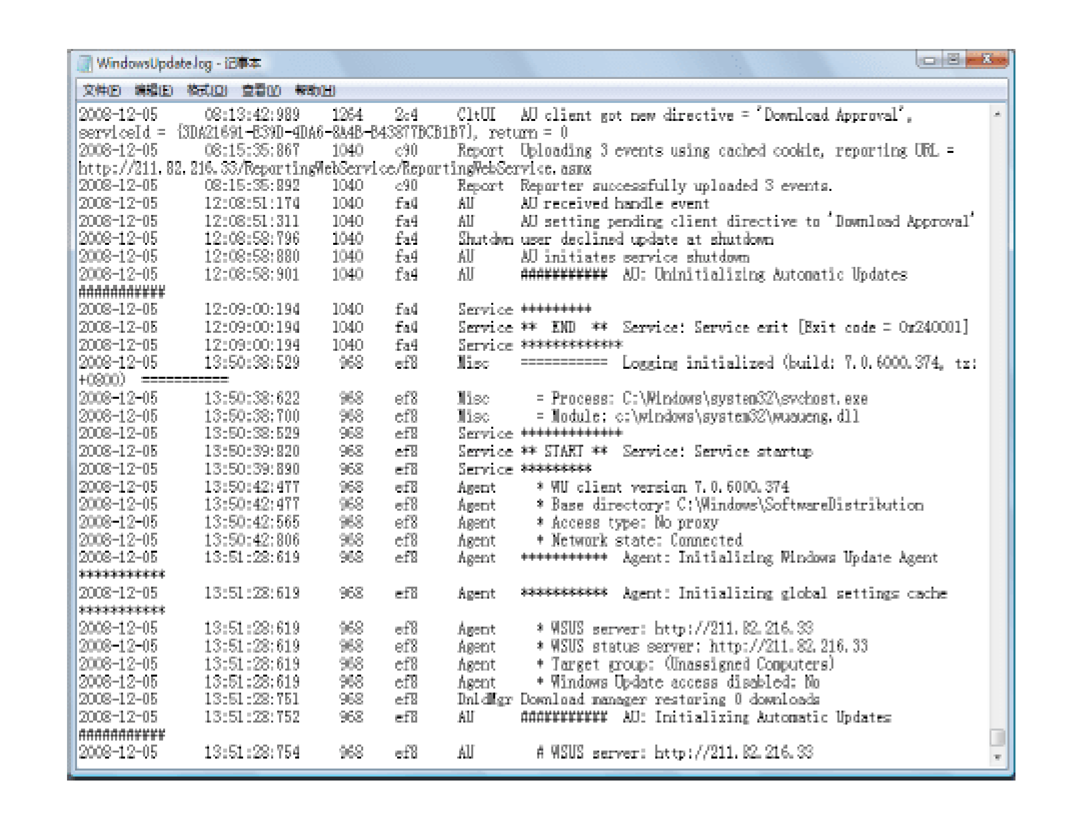


图 3.38　WSUS 客户端更新日志



提示　对于单独客户端而言，至此 WSUS 客户端配置已经完成。但是如果需要在其他同样配置的计算机上部署 WSUS 客户端，逐一配置不仅浪费时间，而且容易出错。此时，可以按照如下步骤导出相关键值，然后在需要部署的计算机上重新导入即可。

04 打开注册表编辑器窗口，依次展开“HKEY_LOCAL_MACHINE”→“SOFTWARE”→“Policies”→“Microsoft”→“Windows”→“WindowsUpdate”分支，右击“WindowsUpdate”并选择快捷菜单中的“导出”选项，将其保存到本地计算机上，如图 3.39 所示。

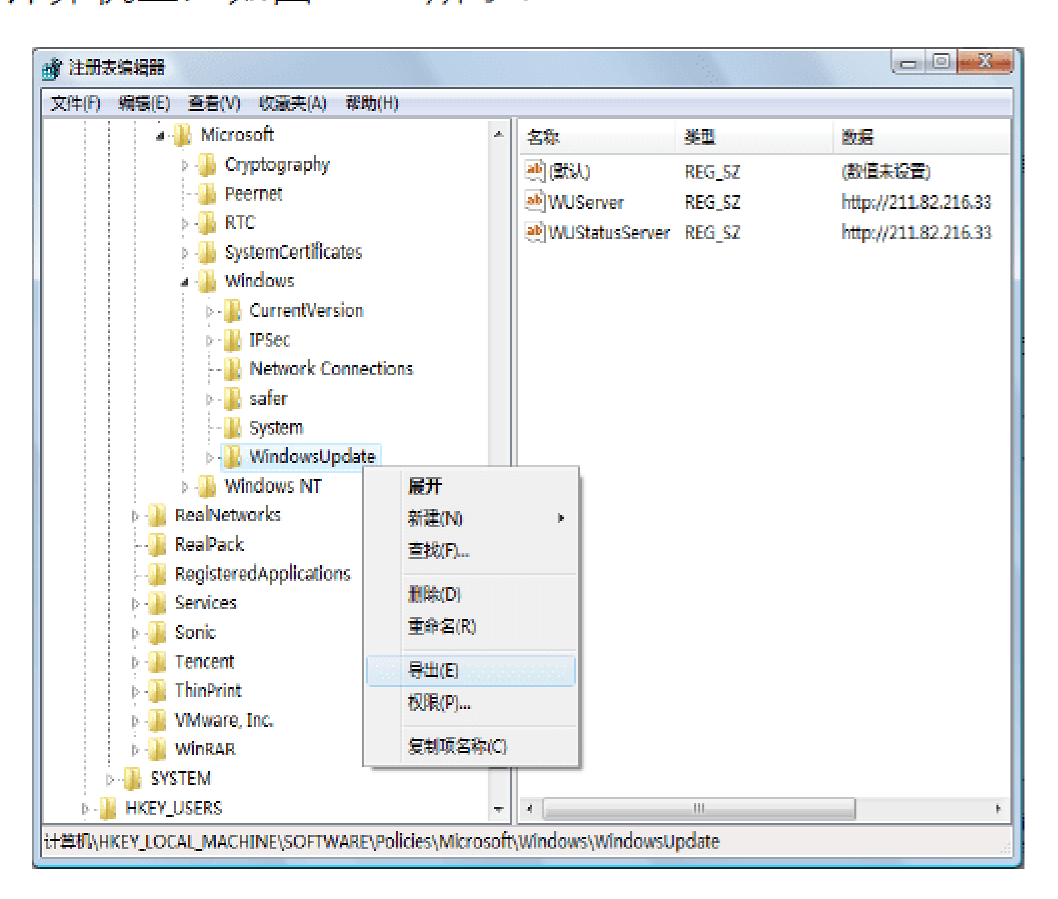


图 3.39　导出注册表键值

05 在其他需要部署 WSUS 客户端的计算机上，双击运行导出的注册表文件，显示如图 3.40 所示“注册表编辑器”对话框。

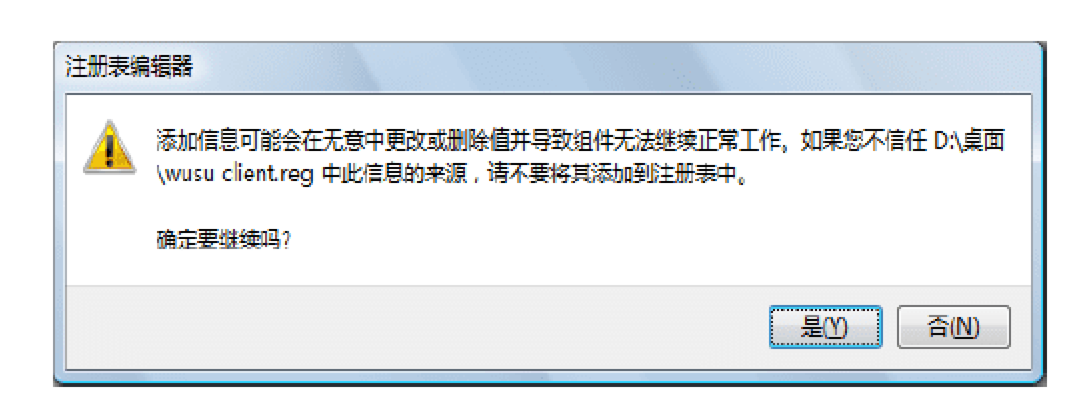


图 3.40　“注册表编辑器”对话框

06 单击“是”按钮即可将其包含的项和值成功添加到注册表中。

小　　结

漏洞在任何操作系统中都是不可避免的，并且会随着用户的不断应用而出现更多的漏洞。系统漏洞并不可怕，关键在于如何预防系统漏洞导致的入侵事件。因此，管理员应该对漏洞的生命周期有所了解，尽量在初期完善各种预防工作，如果已经出现借助漏洞传播的病毒，便难于防范了。发现漏洞后切不可听之任之，必须及时采取相应的修补措施，应对系统漏洞最有效的方法就是指定详细的修补策略，并及时修补漏洞。漏洞除了系统（硬件、软件）本身固有的缺陷之外，还包括用户的不正当配置、管理以及制度上的风险，或其他非技术性因素造成的系统不安全性。修补系统漏洞是发现漏洞后的第一要务，选择一款好用的漏洞修补工具是非常重要的。

习　　题

1. 什么是系统漏洞？简述你遇到过的系统漏洞，总结一下都有哪些特性？
2. 漏洞修补的方法有哪些？
3. 为什么要进行漏洞扫描，选择扫描工具时应注意哪些问题？
4. 简述 MBSA 支持的漏洞扫描模式。

实验：使用 MBSA 扫描 IIS 漏洞

实验目的

熟练运用 MBSA 扫描本地系统和应用程序的漏洞。

实验内容

MBSA 是系统漏洞扫描的必备工具，而 IIS 是最常用的服务组件之一。为确保服务器的安全，应经常对其进行漏洞扫描。

实验步骤

1. 在本地计算机上安装最新版 MBSA 应用程序。
2. 启动 MBSA，在扫描任务中选择检测本地 IIS 组件漏洞。
3. 执行扫描。
4. 查看扫描结果，按照给定的修补方案，及时修改相应配置，或者安装系统补丁。

第4章

活动目录安全

Active Directory 又称活动目录，是 Windows Server 系统中非常重要的服务之一，可用于管理网络中的用户，如计算机、打印机或应用程序等资源。活动目录结构及其数据是 Windows 域中的关键部分，执行恰当的安全和授权措施是非常必要的。在网络中部署 Active Directory 服务，可以对所有网络用户进行逻辑划分，根据不同的身份赋予其相应的访问权限。Windows Server 2008 系统中的活动目录服务，在增强原有特性的同时，增加了许多新功能，如只读域控制器、可重启的活动目录域服务等。

本章导读

- AD DS 安全基本原理
- 有效权限的计算与检索
- 创建信任关系
- 权限委派
- Active Directory 数据库的备份与恢复

4.1 AD DS 安全概述

活动目录域服务（Active Directory Domain Services，简称 AD DS）是 Windows Server 2008 中的新增功能，可以帮助管理员更好地部署安全审核策略、只读域控制器、维护域控制器等。

4.1.1 AD DS 安全基本原理

Windows Server 2008 中的 AD DS 绝非仅仅是名称上的改动，引进这一功能的主要目的就是提升 Active Directory 的安全性。实施活动目录安全措施之前，建议用户对 AD DS 的基本安全原理加以了解，主要包括安全主体、访问控制列表、访问口令、认证和授权。

1. 安全主体

安全主体是所有可以被认证的 AD DS 对象，其中包括用户帐户、计算机帐户等。安全主体是 AD DS 中唯一可以被授权访问资源的对象。

创建安全主体的同时，还会为其分配一个安全标识符（SID），该 SID 在域中是唯一的。将权限委派给用户、组、服务或者计算机，实际上是将权限委派给 SID 的“友好名称”。以用户帐户 liuxh 为例，其“友好名称”为 liuxh。但是 Windows 和 AD DS 都使用与该用户帐户相关的 SID 管理权限和访问控制。管理员更改用户帐户名称时，其 SID 并未发生变化，所以其原有的权限和权利均不会发生变化，使网络管理更加灵活。

SID 由两部分组成：域标识符和相对标识符（RID）。域标识符和域内所有的安全主体相同。RID 在 AD DS 中对每个安全主体来说都是唯一的。SID 都带有前缀 S，表明其是一个安全标识符，末尾是一个相对标识符（Relative Identifier，RID），中间是标志符的子颁发机构（0 个或几个）。安全标识符的第二位是修订版本编号，通常为 1。安全标识符的基本组成如图 4.1 所示。

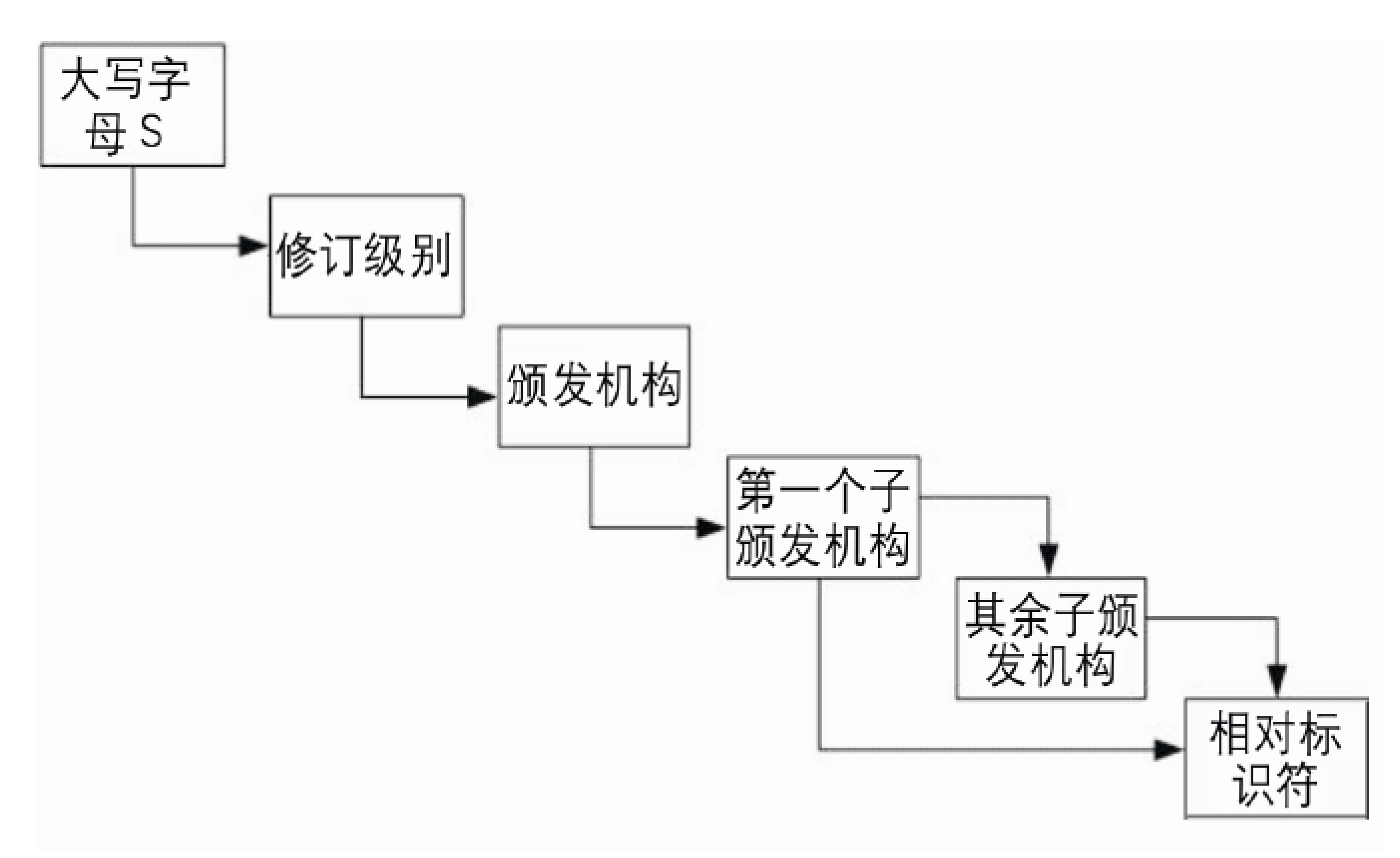


图 4.1　安全标识符的结构和组成部分

安全标识符中，S-1 后面的部分往往会有所不同，但都是以颁发机构代码开始，用于表示

安全标识符的发行机构。表 4.1 中是常用的安全标识符颁发机构代码。

表 4.1　安全标识符颁发机构代码

标识符颁发机构	描　　述
0	SECURITY_NULL_SID_AUTHORITY　用于当颁发机构不可知时
1	SECURITY_LOCAL_SID_AUTHORITY　用于创建代表所有用户的安全标识符，例如，所有用户组的安全标识符是 S-1-1-0，由通用标识符 0 和颁发机构组合而成，其表示所有该机构的用户
2	SECURITY_LOCAL_SID_AUTHORITY　用来创建代表本地终端的登录用户的安全标识符
3	SECRUITY_CREATOR_SID_AUTHORITY　用来创建代表某个对象的创建者或是所有者的安全标识符，例如，文件所有者的安全标识符是 S-1-3-0，其是由创建者或所有者的相对标识符 0 和颁发机构组合而成的；S-1-3-0 用在可继承的访问控制列表中，在继承该列表的子对象里，其会被所有者的安全标识符所代替；S-1-3-1 是文件所有者的安全标识符，其也有同样的作用，不过其安全标识符来自创建者的主要组
5	SECURITY_NT_AUTHORITY　这是操作系统本身；以 S-1-5 开头的安全标识符是由计算机或域发布的，几乎所有这样的安全标识符都有带有 S-1-5

安全描述符的颁发机构还可以包含子颁发机构。在实际应用中，对于内置和预定义安全标识符，仅有 2~3 层子颁发机构；对于其他安全主体的安全标识符，颁发机构的数目限制为 5 个，子颁发机构的限制为 4 层。表 4.2 中列出了常见的子颁发机构。

表 4.2 常见的子颁发机构

子颁发机构	描　　述
5	此安全标识符发布给登录的会话，允许将权限授予特定登录会话下运行的应用程序；这些安全标识符的第一个子颁发机构是 5，基本格式是 S-1-5-5-x-y
6	当一个进程以服务的形式登录，其令牌中就具有特殊的安全标识符；该安全标识符的子颁发机构是 6，基本格式是 S-1-5-6
21	SECURITY_NT_NON_UNIQUE　表示用户或计算机的安全标识符并非是唯一的
32	SECURITY_BUILTIN_DOMAIN_RID　表示内置的安全标识符，例如，内置管理员组的知名安全标识符是 S-1-5-21-544
80	SECUTITY_SERVICE_ID_BASE_RID　表示服务的安全标识符

以如下安全描述符为例：

S-1-5-21-1534169462-1651380828-111620651-500

以 S-1-5 开始，表明其是由 Windows NT 颁发的。第一个子颁发机构是 21，21 表明其是一个 Windows NT 的安全标识符。1534169462、1651380828 以及 111620651 分别是 3 个子办法结构。以 500 结尾，表示是内置管理员帐户的相对标识符。

2. 访问控制列表

访问控制列表主要用于控制网络用户对共享资源的访问，它定义了安全主体对打印机、共享文件夹、组织单位等 AD DS 对象的访问权。访问级别则由委派给安全主体的权限定义。这

些权限被列在对象的 ACL 中。

（1）访问控制列表的分类

访问控制列表有 3 种，分别是随机访问控制列表（DACL）、管理访问控制列表（MACL）和系统访问控制列表（SACL），这 3 种访问控制列表分别用于实现不同的目的。

■ 随机访问控制列表

通常情况下，在 Windows 系统中，如果没有指明访问控制列表类型，都是指随机访问控制列表，他可以由管理员或安全主体所有者创建。例如，管理员可以根据实际需要赋予或收回某个对象的访问权限，就是通过更改随机访问控制列表实现的。

■ 管理访问控制列表

管理访问控制列表（MACL）的主要特征是对所有主体及其所控制的客体（例如：进程、文件、段、设备）实施强制访问控制。为这些主体及客体指定敏感标记，这些标记是等级分类和非等级类别的组合，它们是实施强制访问控制的依据。系统通过比较主体和客体的敏感标记来决定一个主体是否能够访问某个客体。用户的程序不能改变他自己及任何其它客体的敏感标记，这样系统可以防止特洛伊木马的攻击。

管理访问控制列表通常与随机访问控制列表结合使用，并且实施一些附加的、更强的访问限制。一个主体只有通过自主与强制性访问限制检查后，才能访问某个客体。用户可以利用随机访问控制列表来防范其它用户对自己客体的攻击，由于用户不能直接改变强制访问控制属性，所以强制访问控制提供了一个不可逾越的、更强的安全保护层以防止其他用户滥用随机访问控制列表。

■ 系统访问控制列表

系统访问控制列表（SACL）和随机访问控制列表在架构上是一致的，两者的主要区别在于后者赋予或拒绝特定用户和组对该对象的访问权，而前者指定了每个用户或组中要审核的事件。

（2）访问控制项目

访问控制列表主要由两部分组成，分别是访问控制列表大小和访问控制项目（ACE）。ACE 描述与一个特定 SID 有关的访问权限，定义用户或用户组的权限。例如，用户拥有对指定的共享文件夹的读取权限，则该文件夹的 ACL 中就会有一个 ACE 指明该用户拥有读取权限。ACE 的结构如图 4.2 所示。

3 3 2 2 2 2 2 2 2 2 2 2 1 1 1 1 1 1 1 1 1 1
1 0 9 8 7 6 5 4 3 2 1 0 9 8 7 6 5 4 3 2 1 0 9 8 7 6 5 4 3 2 1 0

ACE 大小	ACE 标识	ACE 类型
访问掩码		
SID		

图 4.2　ACE 结构示意图

ACE 的第一部分是 16 位的值，这也是其极限长度。不过，ACE 的长度也不是固定的，因为其包含一个长度不定的 SID。该 SID 定义 ACE 所适用的对象。

3. 访问口令

访问口令主要用于关联安全主体和访问控制列表。用户登录 AD DS 时，安全主体被委派访问口令。访问口令包括用户的 SID、用户所在组的 SID 以及用户的权利和优先级。用户试图获取网络资源的访问，而这些资源已经被委派了 ACL，此时安全子系统会将访问口令信息与 ACL 资源进行对照，确定是否允许安全主体访问。将访问标志的 SID 与 ACL 的 ACE 进行对照，如果匹配，SID 检测权限的级别，然后为安全主体授予权限级别。

4. 认证

认证就是保证访问网络资源的用户身份的过程。用户登录 AD DS 后，首先需要进行身份认证，通过之后，其对应的 SID 和 ACL 将开始执行相应的职能。

当用户从网络计算机登录时，计算机上的 Winlogon 服务装入了 msgina.dll 文件。用户输入密码后，msgina.dll 将信息返回至 Winlogon 服务。Winlogon 服务将信息传递至本地安全颁发机构（LSA）。用户的明文密码非常杂乱，密码的明文副本也被删除。用户名和杂乱密码被传递至安全支持提供程序（SSP）。在 Windows 2000 和更新的版本中，Kerberos 被用作 SSP。然后 SSP 将用户名和杂乱密码发送至域控制器，用于认证。

5. 授权

授权是通过认证后的后续操作，及用户通过 AD DS 认证后，即可被赋予对网络资源的访问权限。

认证过程决定了用户在网络上的权利。如果用户欲访问文件服务器上的文件，并具有正确的权限，则可以访问文件，被授权使用这些文件。如果欲访问打印机服务器上的打印机对象，则授权会再次检测其权限，查看是否可以使用打印机对象。如果不具备，则会被拒绝访问。

4.1.2　只读域控制器

只读域控制器（RODC）是 Windows Server 2008 系统提供的新型域控制器，可以帮助用户在物理安全得不到保证的情况下，部署域控制器并确保其安全性。RODC 包含了活动目录数据库的只读部分，可以帮助用户确保网络环境安全。域控制器是分支机构中最薄弱的环节（参见“第 14 章　分支机构安全”）。使用 RODC，可以将可写域控制器移到合适的数据中心，使用 RODC 替代分支机构中的可写域控制器，从而降低安全风险。

1. RODC 的基本功能

在引入 RODC 之前，分支机构中的用户必须要使用汇接点中的域控制器，通过 Internet 来进行验证。否则，在分支机构中必须要有一个本地域控制器。没有更好的解决办法，因为小型站点不能为可写域控制器提供足够的安全保护。分支机构和汇接站点之间的带宽也非常有限，对于分支机构的用户而言，需要花更多的时间登录，访问网络资源的速度也很慢。在网络中部署 RODC，能够为分支机构提供如下功能：

- 改进的安全性；
- 快速登录；
- 更有效的访问网络资源。

RODC 的主要作用就是弥补域网络中物理安全的漏洞，既保证了客户端快速可靠地身份验证，同时还保证了可写域控制器数据的安全。在某些特殊域环境中，管理员还可以使用 RODC 灵活掌控可写域控制器的安全。例如，需要在域控制器上安装应用程序时，程序所有者必须交互登录到域控制器上，或是使用终端服务来设置和管理应用程序，这可能会为可写域控制器带来安全风险。存储所有域用户密码的地方，也可能存在漏洞，例如，企业内部网或是面向程序角色。RODC 的主要用途之一，就是部署在分支机构中，为其提供物理安全防护和基本身份验证。

2. 只读 AD DS 数据库

除帐户密码之外，RODC 保存了可写域控制器所保留的所有活动目录对象和属性。但是，不能对其数据库进行更改。RODC 数据库的更新过程是通过复制可写域控制器数据库完成的，管理员只能对可写域控制器数据库进行修改和存储。

请求对目录读取访问的本地应用程序可以获取访问权限。请求写入访问的轻型目录访问协议（Lightweight Directory Access Protocol，LDAP）应用程序将接收 LDAP 引用响应。此响应将其定向到可写域控制器，在这里可以被访问。

3. RODC 筛选的属性集

在 RODC 筛选的属性集中定义的属性不允许复制到林中的任何 RODC 上，对于需要使用 AD DS 存储数据（例如，密码、凭据或加密密钥）的应用程序，并且不希望将数据存储到 RODC 上（以防泄露），则可以将这组属性定义为域对象中筛选属性集的一部分，该属性集不会复制到任何 RODC 上。

恶意用户可以尝试采用上述方式对其进行配置，以试图复制在 RODC 筛选的属性集中定义的属性。如果 RODC 尝试从运行 Windows Server 2008 的域控制器复制这些属性，则复制请求会被拒绝。但是，如果 RODC 尝试从运行 Windows Server 2003 的域控制器复制属性，则复制请求可能成功。如果计划使用 RODC 筛选的属性集，必须确保林功能性级别是 Windows Server 2008，则运行 Windows Server 2003 的域控制器就无法存在于林中，从而确保 RODC 的安全。

为防止错误设置 AD DS 的功能，建议不要将系统关键属性添加到 RODC 筛选的属性集中。AD DS 正常工作所需要的属性即为系统关键属性，包括本地安全机构（Local Security Authority，LSA）、安全帐户管理器（Security Accounts Manager，SAM）和微软特定的安全服务提供程序接口（Security Service Provider Interfaces，SSPI）。系统关键属性的 schemaFlagsEx 属性默认值等于 1。

RODC 筛选的属性集应在保存架构操作主机角色的服务器上进行配置。当架构主机运行 Windows Server 2008 系统时，如果尝试将系统关键的属性添加到 RODC 筛选集，则服务器将返回“unwillingToPerform”LDAP 错误。如果尝试将系统关键的属性添加到在 Windows Server 2003 架构主机上的 RODC 筛选的属性集，则操作过程中虽然没有报告错误，但并不能成功添加。因此，在将属性添加到 RODC 筛选集时，建议架构主机为 Windows Server 2008 域控制器，

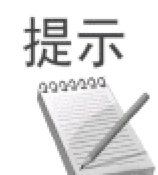
以确保在 RODC 筛选的属性集中不包括系统关键的属性。

管理员可以通过查看 Windows Server 2008 安装光盘上的相关文件，详细了解 Windows Server 2008 的默认架构。

4. 单向复制

由于不会将更改直接写入 RODC，所以也就不会产生来自 RODC 的更改，作为复制伙伴的可写域控制器，也就不必从 RODC 导入更改。这意味着恶意用户在分支位置可能进行的任何更改或损坏，都不能从 RODC 复制到林的其余部分，也就减轻了复制拓扑中桥头服务器的工作负荷以及监视复制所需开销。

提示



桥头服务器是站点中被指定用于完成与林中其他站点之间信息复制的服务器。

RODC 单向复制适用于 AD DS 和分布式文件系统（Distributed File System，DFS）复制。RODC 对 AD DS 和 DFS 复制更改执行标准入站复制。

5. 只读 DNS

如果在网络中部署了 RODC，则建议在 RODC 所在分支机构中同时部署 DNS 服务器，以便为本地用户提供快速身份验证，否则本地用户的身份验证请求仍需通过 Internet 传输到可写域控制器上完成。要为分支机构提供名称解析，可以在 RODC 运行 DNS 来复制 DNS 使用的所有应用程序目录分区包括 ForestDNSZones 和 DomainDNSZones。如果已在 RODC 上安装了 DNS 服务器，则客户端可以与查询任何其他 DNS 服务器一样，查询该 DNS 服务器以进行名称解析。

但是，RODC 上的 DNS 服务器不直接支持客户端更新。因此，RODC 不为其承载的任何活动目录集成区域注册名称服务器（Name Server，NS）资源记录。当客户端尝试根据 RODC 更新其 DNS 记录时，服务器会返回一个引用。然后客户端可以尝试对引用中提供的 DNS 服务器进行更新。在后台中，在 RODC 上的 DNS 服务器尝试从进行更新的 DNS 服务器复制更新记录。此复制请求仅适用于单个对象（DNS 记录）。在此特殊复制单个对象请求过程中不会复制更改区域或域数据的完整列表。

4.1.3　可以重启的 AD DS

在日常管理中，某些操作通常需要重启域控制器才可以生效，例如安装部分安全更新之后。使用可重启的 AD DS 就可以无需重启域控制器而执行这些操作。此外，管理员还可以停止 AD DS，以执行活动目录数据库脱机碎片整理等任务。另外，可重启的 AD DS，还允许管理员在服务器上运行不依赖 AD DS 的服务器角色（如 DHCP），在进行安全升级或脱机碎片整理时仍可用来应答客户端请求。

默认情况下，可重新启动的 AD DS 在运行 Windows Server 2008 的所有域控制器上都是可用的。使用此功能不存在任何功能级别的要求或任何先决条件，与其他服务一样，可以使用

MMC 控制台管理单元或命令行来停止和重新启动 AD DS。需要注意的是，如果停止了 ADDS，则 DNS、KDC 以及站间消息传递服务也会停止。

停止 AD DS 与在目录服务恢复模式中登录 AD DS 相似，但是可重新启动的 AD DS 为运行 Windows Server 2008 的域控制器提供了一种新的状态——AD DS 停止。在此状态下，域控制器与目录服务恢复模式和域成员服务器的特性类似。在目录服务还原模式时，位于本地域控制器上的活动目录数据库（Ntds.dit）处于脱机状态。如果其他域控制器可用，本地域控制器可以使用其进行登录。如果无法联系到其它域控制器，可以使用“目录服务还原模式密码”登录。作为成员服务器，该服务器被加入域，组策略或者其他设置仍被应用到计算机，但其无法为登录请求服务或者与其它域控制器进行复制操作。

4.1.4 AD DS 审核

在 Windows Server 2008 中，用户可以通过建立 AD DS 审核来记录新旧属性值，当活动目录对象及其属性发生变化时，将自动生成相应的系统事件。AD DS 审核同样适用于 Active Directory 轻量目录服务（AD LDS，Active Directory Lightweight Directory Services）中。全局审核策略审核对目录服务的访问控制，无论针对目录服务事件的审核是被启用或被禁用，该安全选项决定了当确定的操作被应用到目录对象时，相应的事件都将被记录到安全日志中。

在 Windows 2000 Server 和 Windows Server 2003 中，只有一个审核策略“审核目录服务访问”，用以控制目录服务事件审核的启用和禁用。在 Windows Server 2008 中，该策略分为四个子类别：

- 目录服务访问；
- 目录服务更改；
- 目录服务复制；
- 详细的目录服务复制。

要审核对象的更改，应启用子类别对象服务更改审核策略，其对应的安全事件 ID 及描述信息如表 4.3 所示。

表 4.3 AD DS 操作

类型	事件 ID	描述
修改	5136	成功修改属性后记录
创建	5137	创建对象后记录
恢复	5138	恢复对象后记录
移动	5139	移动对象后记录

4.1.5　活动目录数据库装载工具

微软提供了一种方法，可以比较不同时间获取的存在于快照或备份中的数据，从而改进活动目录的恢复过程。这从安全的角度来讲是非常重要的，因为其提供了一种追踪安全缺口出现之前所出现的变化的方式——一种通过比较数据进行区分的方式。未达到这一目的，可以使用新的活动目录数据库装载工具（Dsamain.exe），其有助于决定在数据丢失后要还原哪些数据。这样就无需还原多个备份也可以比较其中包含的活动目录数据。

注意



该功能在发展的过程中，所使用的代码名有“快照查看器”和“活动目录数据库装载工具”，在一些文档中仍然可以看到这些名。

首先要了解活动目录数据库装载工具本身并不会自动恢复删除的对象，它有助于简化恢复意外删除对象的过程。在 Windows Server 2008 之前，当对象或组织单元（OU）被意外删除时，精确确定哪些对象被删除的唯一方法就是从备份中还原数据。这种方法存在缺点：必须重启 DCRS 中的域控制器才能执行授权还原，除非将备份还原到不同域控制器，否则管理员无法比较在不同时间点获得的备份中的数据。

活动目录数据库装载工具的用途是公开存储在快照或联机备份中的 AD DS 数据。然后，管理员可以比较不同时间点获得的快照或备份中的数据，进而可帮助管理员更好地决定还原哪些数据而无需使服务中断。使用活动目录数据库装载工具可以将删除的 AD DS 或活动目录轻型目录服务（Active Directory Lightweight Directory Services，AD LDS）数据以通过卷影复制服务（Volume Shadow Copy Service，VSS）获得的 AD DS 快照进行保留。该工具不会真正的恢复删除的对象和容器。作为后续步骤，管理员必须执行数据恢复。

由于备份包含敏感数据，所以将备份保存为只读形式，而对于 AD DS 快照，应当只允许域管理员组或企业管理员组的成员使用轻型目录访问协议（LDAP）工具（例如 Ldp.exe）查看快照。建议使用加密或其它数据保护，以保证 AD DS 快照不受未经授权的访问。

使用活动目录数据库装载工具的过程包括下列步骤：

- 虽然不是必需，但仍然建议计划任务定期运行 Ntdsutil.exe 获取包括 AD DS 数据库的卷的快照；
- 运行 Ntdsutil.exe 列出所有快照，然后装载要查看的快照；
- 运行 Dsamain.exe 作为 LDAP 服务器公开快照卷。例如，若要查看默认路径中的近期快照，其命令为：dsamain–dbpath c:\$snap_200711201220_volumec$\windows\ntds\ntds.dit –ldapport 41389 这样就可以在端口 41389 上，通过 Ldp.exe 得到快照。

Dsamain.exe 使用的参数如下：

- AD DS 数据库（Ntds.dit）路径。默认情况下，该路径打开为只读，但必须是 ASCII；
- 日志路径。该路径可以是临时路径，但必须具有写入权限；
- 4 个端口号为 LDAP、LDAP-SSL、Global Catalog 和 Global Catalog－SSL。只有 LDAP 端口是必需的。如果未指定其他端口，将分别使用 LDAP+1、LDAP+2 和 LDAP+3。

例如，如果指定 LDAP 端口 41389 而未指定其他端口值，则默认情况下 LDAP-SSL 端口将使用端口 41390，以此类推；

- 运行 Ldp.exe 并将其连接到在之前的步骤中作为 LDAP 服务器公开快照时指定的快照的 LDAP 端口；
- 和使用所有实时域控制器一样浏览快照。可以在“命令提示符”窗口按 Ctrl+C Dsamain，或者如果远程运行该命令，则可以通过设置 rootDSE 对象的 stopservice 属性停止 Dsamain。

如果了解了哪些 OU 或对象被删除，可以在快照中查找已删除对象并记录属性和属于已删除对象的返回链接。使用逻辑删除恢复功能恢复这些对象。然后，使用和快照中相同的去除的属性和返回链接，手动重新填充这些对象。虽然必须手动重新创建去除的属性和返回链接，但活动目录数据库装载工具可以重新创建删除的对象及其返回链接，而无需以目录服务还原模式重启域控制器。还可以使用该工具查看以前的 AD DS 配置，包括已生效的权限，这对恢复工作会大有帮助。在 AD DS 停止时，若想知道上次工作时其是怎样配置，此特性也是非常有用的。

4.1.6 AD DS 部署安全

通常情况下，多数用户都是使用默认方式安装服务器操作系统的，并且几乎未经任何安全设置就投入使用，其实这中做法本身就存在非常严重的安全隐患。Windows 操作系统的默认安装方式适用于大多数普通用户，许多安全功能并未启用，如果在此基础上部署 AD DS 无疑会增加域控制器的风险。管理员可以从以下几个方面确保 AD DS 的部署安全。

1. 安全的操作系统

操作系统是网络服务的根本。管理员可以通过如下设置打造安全的服务器操作系统：

- 使用 NTFS 文件系统格式化驱动器。Windows 系统中许多安全功能的部署和实现，都是基于 NTFS 文件系统的，因此，建议使用 NTFS 文件系统格式化服务器的所有磁盘分区；
- 只安装 TCP/IP 协议。通常情况下，在服务器上只安装 TCP/IP 协议就足够了，既可以满足基本的网络应用，又能减少被攻击的机率；
- 安全 DNS。保证提升域控制器之前已经安全的安装和配置了 DNS 服务器；
- 不安装 IIS。默认情况下，Windows Server 2003 和 Windows Server 2008 并不安装 IIS 服务，或将其作为操作系统的一部分。在应用过程中，同样应注意避免在域控制器上部署 IIS 服务。

2. 安全的安装位置

确保域控制器的安装位置安全。Dcpromo 使用的自动安装文件和自动提升文件中包括管理员帐户提升域控制器时使用的密码。如果使用的是高级版本的 Dcpromo，则完成域控制器提升后，应从系统缓存中删除安装文件。系统状态只对墓碑式生命周期有效，Dcpromo 不使用过期的系统状态。

3. 系统用户帐户安全

入侵者攻击服务器时，首先需要假设一个用户帐户并猜测其可能的密码，而 Windows 系统中的Administrator和Guest帐户是使用频率最高的用户帐户之一。虽然这些帐户不能被删除，但是可以通过重命名的方式，避免由此导致的网络攻击。Guest 帐户默认是被禁用的，对于服务器而言，建议管理员不要启用该帐户。对于 Administrator 帐户而言，建议管理员部署 AD DS 之后，立即更改管理员帐户名称。

保护管理员帐户还有另一种方法，那就是创建一个新帐户，使其具有所有相同的权限，然后禁用内置管理员帐户。网络上的许多程序都会自动扫描系统上管理员的 SID。前面也曾提到，可以对帐户进行重命名，但是 SID 不会任何变化。内置管理员 SID 都是以 500 结尾，网络上的程序可以很轻松地找出这些 SID。

4. 使用 Syskey 保护密码信息

所有域密码都被保存在 AD DS 数据库中。如果域控制器遭遇物理攻击，则 AD DS 数据库的安全也就难以保证。为此，管理员可以使用 Syskey 加密密码。Syskey 的安全保护级别有 3 种：

- 等级 1。默认情况下，Windows 2003 和 Windows Server 2008 启用的是等级 1，即系统密码会自动生成，加密密码保存在本地服务器上；
- 等级 2。与等级 1 的操作方法相同，但是启动计算机时，管理员可以选择额外的密码输入系统。与等级 1 不同，额外密码不保存在本地服务器上，可以保存在 U 盘或软盘上；
- 等级 3。登录过程中要求更多的管理员互动操作。计算机自动生成密码，并保存在软盘上。启动时，如果管理员没有将软盘放进系统，则计算机不能启动。

4.1.7　活动目录轻型目录服务

通过使用 Windows Server 2008 Active Directory 轻型目录服务（Active Directory Lightweight Directory Services，AD LDS）角色，可以为已启用目录的应用程序提供目录服务，而无需占用域和林中的开销，并且不要求在整个林中只使用一个架构。

1. AD LDS 概述

Active Directory 轻型目录服务在 Windows Server 2008 之前，被称作 Active Directory 应用模式（Active Directory Application Mode，ASAM），可以提供目录服务，用于为已启用目录的应用程序提供目录服务，而无需占用域和林中的空间，并且不要求在整个林中只使用一个架构。

AD LDS 是一个轻型目录访问协议（LDAP），没有 AS DS 所必需的依存关系。AD LDS 提供的许多功能都与 AD DS 相同，但是无需部署域或域控制器。用户可以在一台计算机上同时运行多个 AD LDS 实例，每个 AD LDS 实例都有独立管理的架构。这样就可以将 AD LDS 隔离，使其仅为单个程序所用。从系统安全角度考虑，可以在一台服务器上部署多个 AD LDS 实例，并且这些实例不互相连接，也不共享任何信息。

AD LDS 为已启用目录的应用程序和 Windows 服务器操作系统提供目录服务，其存储网

络架构、用户、组和网络服务的核心信息。在此角色下，AD DS 在整个林中必须遵循单一架构。AD LDS 必须在整个林中 AD LDS 不需要或不依赖 Active Directory 域或林。但是，在有 AD DS 的环境中，AD LDS 可以使用 AD DS 对 Windows 安全主题进行身份验证。使用 AD LDS 服务器角色，能够为已启用目录的程序提供不依赖活动目录林的目录服务。如果已经有了 AD DS，则可以将其用于 Windows 安全主题的验证。例如，程序需要扩展架构，但由于某些原因无法实现，则可以扩展 AD LDS 架构并存储信息，用户也可以使用 AD DS 验证并连接到程序，AD LDS 负责存储特定程序的值。

2. Windows Server 2008 中 AD LDS 新特性

Windows Server 2008 操作系统的 AD LDS 新特性如下：

- 审核 AD LDS 的更改。可以使用新的审核子类别来设置 AD LDS 审核，以便在对对象及其属性进行更改时记录旧值和新值；
- 数据库装载工具与 AD DS 中的数据装载工具工作方式相同。借助此功能，无需重新启动服务器，即可查看联机存储在不同时间点获取的快照中的目录数据，以便更好地决定要还原的数据；
- 支持 Active Directory 站点和服务。若要使用该工具，必须导入 MS-ADLDS-DisplaySpecifiers.LDF 中的类，以扩展要管理的配置集架构。借助此功能，可以使用活动目录站点和服务管理单元来管理 AD LDS 实例之间的复制；
- 实例设置过程中的 LDAP 数据交换格式（LDAP Data Interchange Format，LDIF）文件的动态列表。借助此功能，除了随 AD LDS 一起提供的默认 LDIF 文件外，还可以通过将自定义 LDIF 文件添加到%systemroot%\ADAM 目录中，使自定义 LDIF 文件可用于 AD LDS 实例设置过程中；
- 递归链接属性查询。借助此功能，可以创建跟踪嵌套属性链接的单个 LDAP 查询。对于确定组成员身份和体系，该功能非常有用。

4.2　有效权限的计算与检索

在实际应用中，由于不同权限之间的优先级不同，并非赋予的所有权限都是有效的。例如，管理员赋予某用户帐户远程访问的权限，但禁止该用户所在组进行远程访问，则此时该用户仍不能远程登录服务器。通过有效权限计算器可以了解指定对象拥有哪些有效权限。由于有些权限是必须在用户登录后方可拥有的，而有效权限计算器只能计算已登录用户的权限，因此，计算结果显示的指示对象拥有权限的近似值。

4.2.1　有效权限计算规则

有效权限计算按照如下安全标识符来完成计算：



- 全局组成员身份；
- 本地组成员身份；
- 本地权限；
- 本地特权。

有效权限计算不会考虑这些安全标识符：

- 匿名登录；
- 批处理和创建者组；
- 拨号；
- 企业域控制器；
- 交互；
- 网络；
- 代理；
- 受限；
- 远程；
- 服务；
- 系统；
- 终端服务器用户；
- 其他组织；
- 此组织。

4.2.2　检索有效权限

准确检索上述信息需要读取成员身份信息的权限。如果指定用户或组是域对象，则必须具有读取该域上对象的组信息的权限。以下是一些相关的默认域权限：

- 域管理员具有读取所有对象上的成员身份信息的权限；
- 工作站或独立服务器上的本地管理员，不能读取域用户的成员身份信息；
- 当域处于 Windows 2000 以前版本的兼容模式下时，域用户只能读取成员身份信息；
- 用户或组的有效权限用灰色的勾号表示，且不能更改。

以域控制器上的共享文件夹“share”为例，通过如下操作即可查看用户帐户“liuxh”对该文件夹拥有的有效权限。

---

01 在“Active Directory 用户和计算机”窗口中，右击“share”文件夹并选择快捷菜单中的“属性”，打开“share 属性”对话框，切换至“安全”选项卡，单击“高级”按钮打开“share 的高级安全设置”对话框，切换至“有效权限”选项卡。单击“选择”按钮，显示如图 4.3 所示“选择用户、计算机或组”对话框，在“输入要选择的对象名称”文本框中，输入用户或组的名称。

02 单击“确定”按钮，系统进行后台权限计算，完成后显示如图 4.4 所示结果。选中的复选框表示用户或

组对该文件或文件夹的有效权限，如果复选框背景颜色为灰色，表示该权限是从其父文件夹继承的。

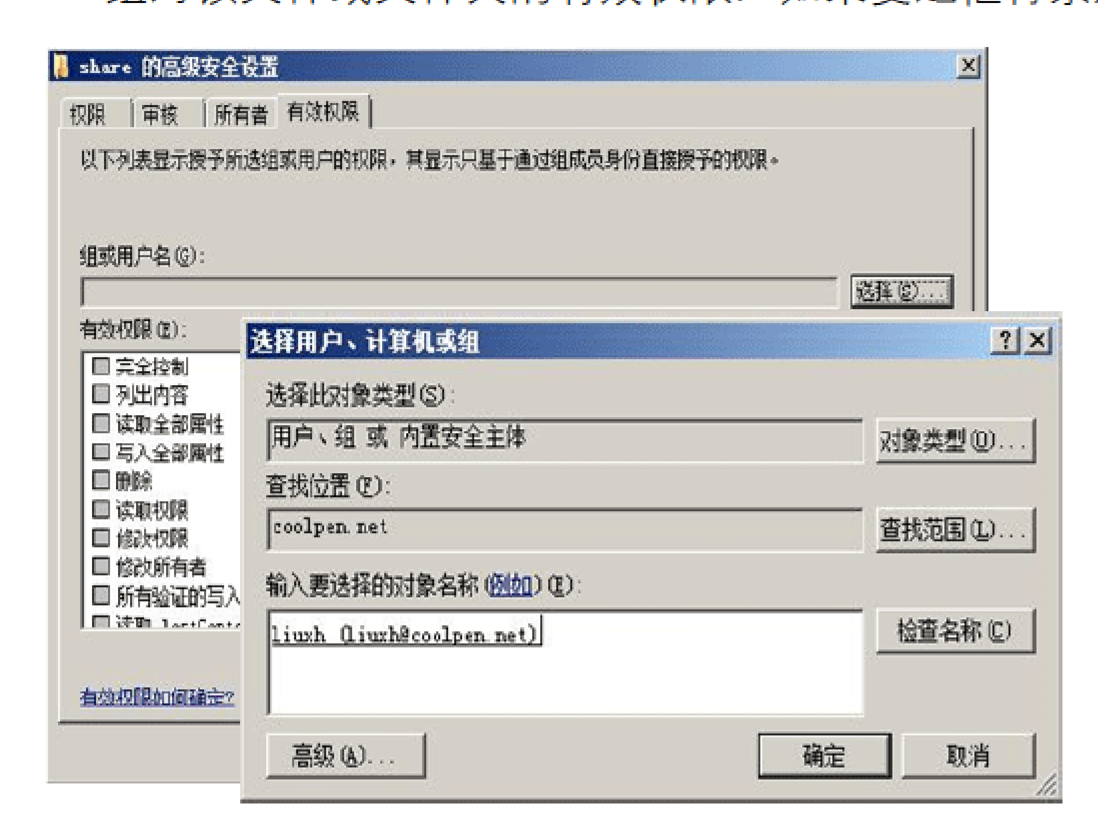


图 4.3　选择用户、计算机或组

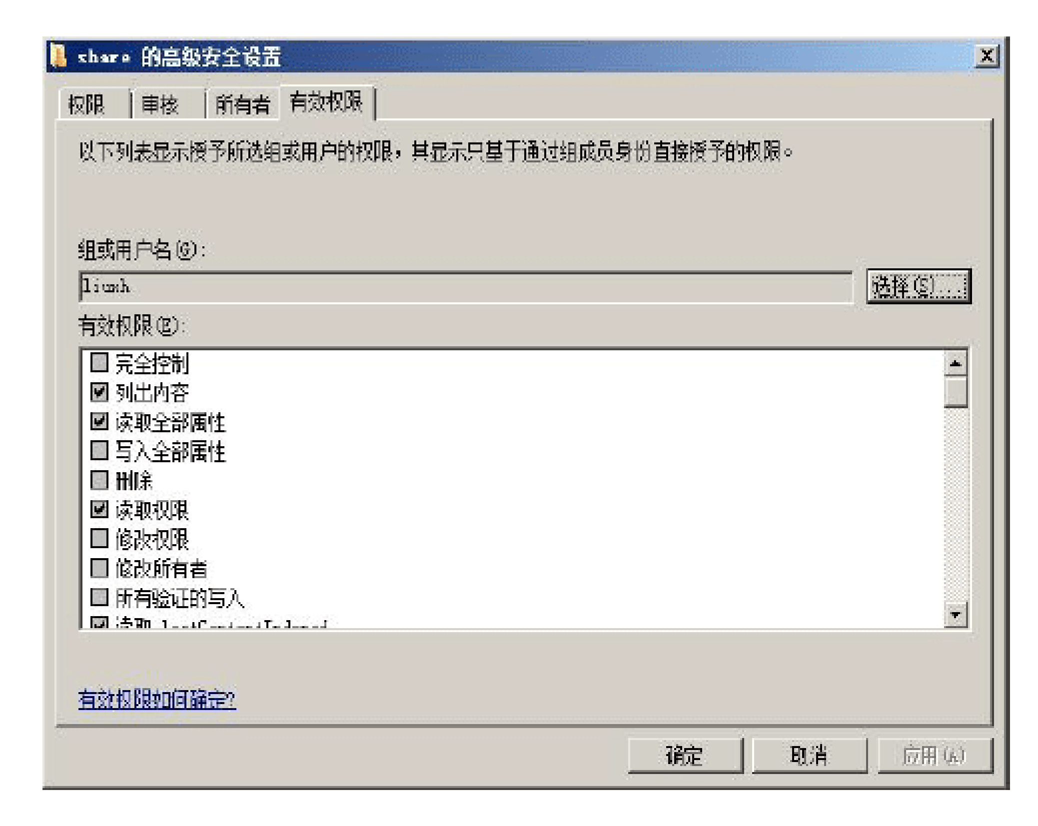


图 4.4　liuxh 用户对“share”共享文件夹的有效权限

4.3　创建信任关系

域本身就是定义网络安全边界的，因此默认情况下，不同域之间是不存在任何联系的，并且无法实现资源共享。在大型网络环境中，存在多个相互独立的域，但有时又需要实现彼此之间的资源共享，此时就需要创建域之间的信任关系，是双方域用户可以交互登录、访问对方的共享资源。

4.3.1　信任关系概述

域之间的相互隔离就是为了确保网络的安全，创建信任关系之后，无疑会扩大网络边界，增加网络安全风险。因此，创建信任关系之前，管理员必须对信任关系类型、方向等相关特性有所了解，并进行详细的规划，在实现互访的同时确保网络的安全。

1. 信任关系的传递性

信任关系的传递性决定信任关系是否可扩展到建立信任的两个域之外，按照是否具有可传递性，信任关系分为可传递信任和非传递信任。可传递信任用于将信任关系扩展到其他域，而非传递信任用于拒绝与其他域之间的信任关系。

（1）可传递信任

任何一个 Windows Server 2008 或 Windows Server 2003 域被加入到域目录树后，这个域会自动信任其父域，同时父域也会自动信任这个新域，并且这些信任关系是可以传递到以后加入到目录树中的其他域的。可传递信任关系将以域树形成时的

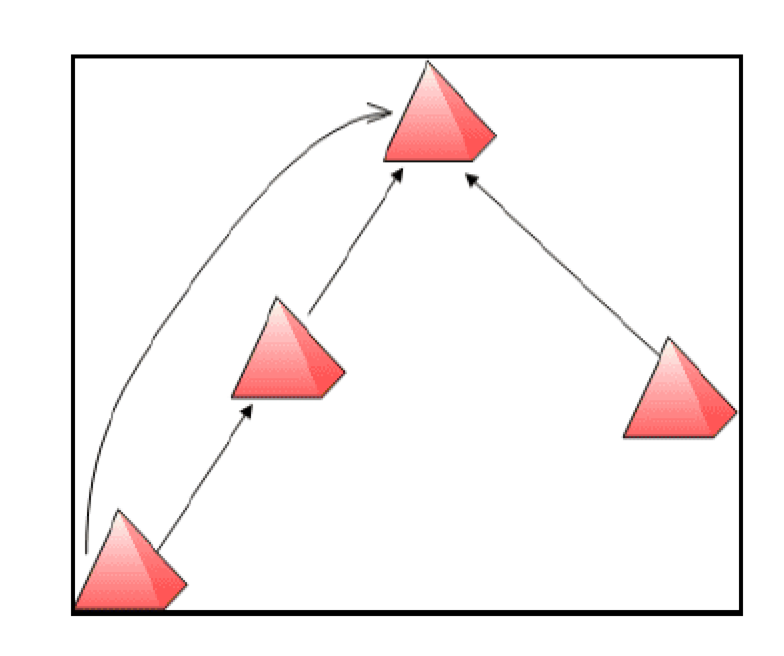
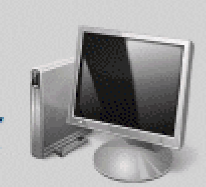


图 4.5　可传递信任关系



方向沿域树向上流动，最终在域树中的所有域之间创建可传递信任。如图 4.5 所示是可传递信任关系及访问示意图。

由于这种信任关系都是建立在父域和子域之间的，所以也被称为父子信任关系。除了这种方式默认创建的可传递信任关系外，还可以通过手动方式创建如下 3 种类型的可传递信任关系：

- 快捷信任：在相同域目录树或域目录林中的域之间的可传递信任，用于缩短大型复杂的域树或林中的信任路径；
- 林信任：在林根域和第 2 个林根域之间的可传递信任；
- 领域信任：在 Active Directory 域和 Kerberos V5 领域之间创建可传递信任。

（2）非传递信任

非传递信任受信任关系中的两个域的约束，并不流向林中的任何其他域。此时用户也将无法访问到没有直接建立信任关系的域，如图 4.6 所示。

非传递域信任是以下各项之间唯一的信任关系形式：

- Windows Server 2008 域、Windows Server 2003 域、Windows NT 域彼此之间；
- 一个林中的 Windows Server 2008 域和其他林中的某个域（当没有被林信任连结时）。

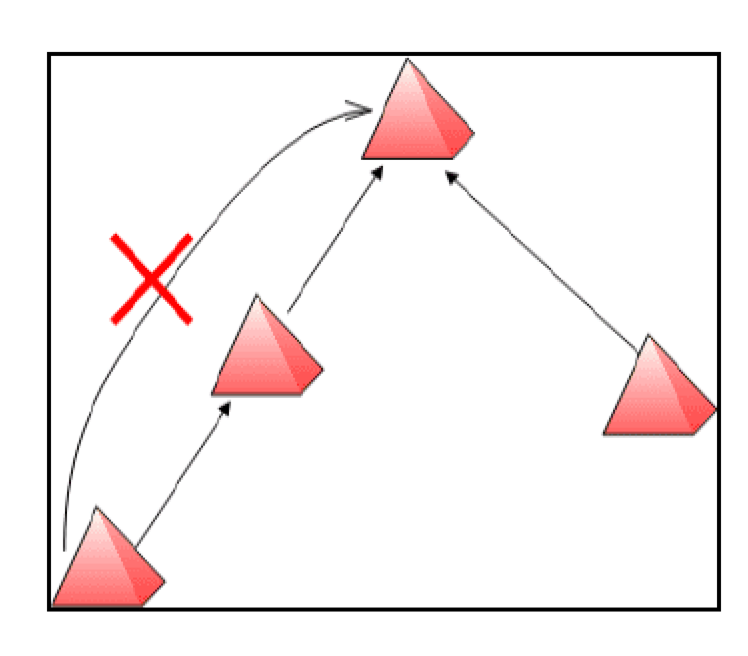


图 4.6　非传递信任关系

管理员可以使用手动方式创建下列非传递信任：

- 外部信任。在单个 Windows 域之间，或不同林的 Windows 域之间创建的非传递信任关系；
- 领域信任。在 Windows Active Directory 域和 Kerberos V5 领域之间的非传递信任。

2. 信任方向

“信任域”和“受信任域”是信任关系中的两个主体，信任方向就是决定彼此之间的信任方式，通常以箭头表示。信任方向的分配将直接影响到用于身份验证的路径，信任路径则是身份验证请求必须符合域之间的一系列信任关系。信任方向可以分为单向信任和双向信任。

（1）单向信任

单向信任是两个域之间创建的单向身份验证路径，即受信任域中的用户帐户可以使用信任域上的身份验证方式，并访问域中的资源，反之则无法实现。如图 4.7 所示是单向信任关系示意图。

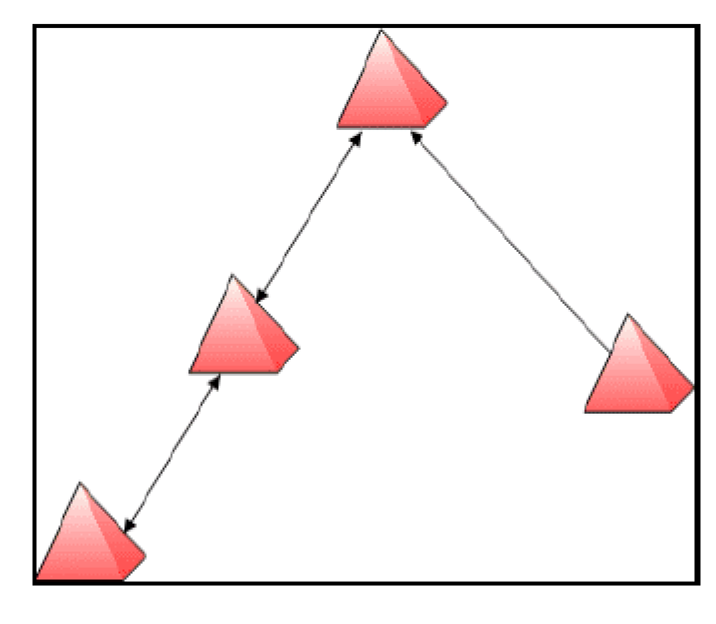


图 4.7　单向信任

（2）双向信任

默认情况下，Windows Server 2008 和 Windows Server 2003 林中的所有域信任关系都是双向、可传递的。创建新的

子域时，双向可传递信任在新的子域和父域之间自动建立，这意味着身份验证求可按两种方向在两个域之间传递。如图 4.8 所示为双向信任关系示意图。

Windows Server 2003 可以建立与下列各域之间的单向或双向信任：

- 同一林中的 Windows Server 2003 域；
- 不同林中的 Windows Server 2003 域；
- Windows NT 4.0 域；
- Kerberos V5 领域。

图 4.8　双向信任关系

3. 信任安全规划

在默认状态下，在使用“Active Directory 安装向导”创建域的同时，系统会自动创建默认的信任关系，父子信任和域间信任。除此之外，用户根据需要创建信任关系之前，必须做好详细规划，以免实施之后导致不必要的网络安全威胁，通常应考虑如下因素：

（1）何时创建快捷信任

快捷信任是当系统管理员需要优化身份验证过程时，可以使用单向或双向可传递信任。身份验证要求必须首先通过域树之间的信任路径，在复杂的林中，验证的时间会很长，执行的效率会很低。快捷信任可以缩短该信任验证的时间。信任路径是为了传递任何两个域之间的身份验证而必须遍历的一系列的域信任关系。

当某个域中经常有许多用户登录林中的其他域时，有必要使用快捷信任。快捷信任可有效地缩短两个不同树中的域之间进行身份验证所要经过的路径。

- 使用单向信任：建立在不同域树中的两个域之间的单向快捷信任，可以减少完成身份验证求所需的时间，但只能在一个方向上传递；
- 使用双向信任：建立在不同域树中的两个域之间的双向快捷信任，可以减少完成源自其中任一域的身份验证求所需的时间。

（2）何时创建林信任

只能在一个 Windows Active Directory 林的林根域和另一个 Windows Active Directory 林的林根域之间创建林信任，此时可以为目录林中的所有域控制器提供一种单向或双向的可传递信任关系。

- 使用单向林信任：两个林之间的单向林信任允许受信任林的成员使用信任林中的资源，但此信任只是单向的；
- 使用双向林信任：两个林之间的双向林信任允许任一个林的成员使用另一个林中的资源；每个林中的域隐式信任另一个林中的域。

为保证网络的安全，默认情况下，域与域之间是无法正常互访的，同一个域中的用户无法访问另一个域。域中的用户要想自由访问网络中的各个服务器（不管是否属于这个用户属于的域），需要在不同域间创立信任关系。

4.3.2　创建域间信任关系

1. 网络参数设置

在创建双向信任关系之前，以域管理员身份登录域控制器，打开“Internet 协议版本 4（TCP/IPv4）属性”对话框，将当前域控制器的“首选 DNS 服务器”的 IP 地址指向目标域 IP 地址“192.168.1.95”，如图 4.9 所示。

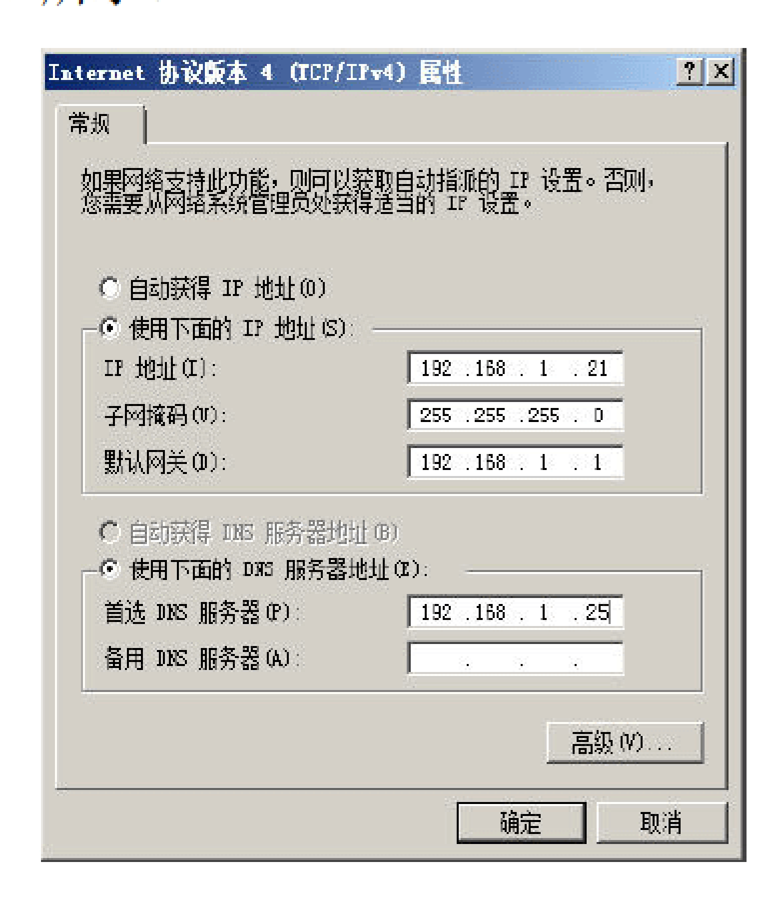


图 4.9　“Internet 协议版本 4（TCP/IPv4）属性”对话框

2. 创建信任关系

本案例的实验环境中包括两台彼此独立的域控制器 coolpen.net 和 hsnc.cn，IP 地址分别为 192.168.1.21 和 192.168.1.25。在其中一台域控制器（本例为 coolpen.net）上执行如下操作。

01 依次选择“开始”→“管理工具”→“Active Directory 域和信任关系”选项，显示如图 4.10 所示“Active Directory 域和信任关系”窗口。

02 右击域名 coolpen.net，选择快捷菜单中的“属性”选项，打开“coolpen.net 属性”对话框，单击“信任”切换至如图 4.11 所示“信任”选项卡。目前，该域中包含一个子域 hengshui.coolpen.net，自动创建了信任关系，所以显示在列表中。

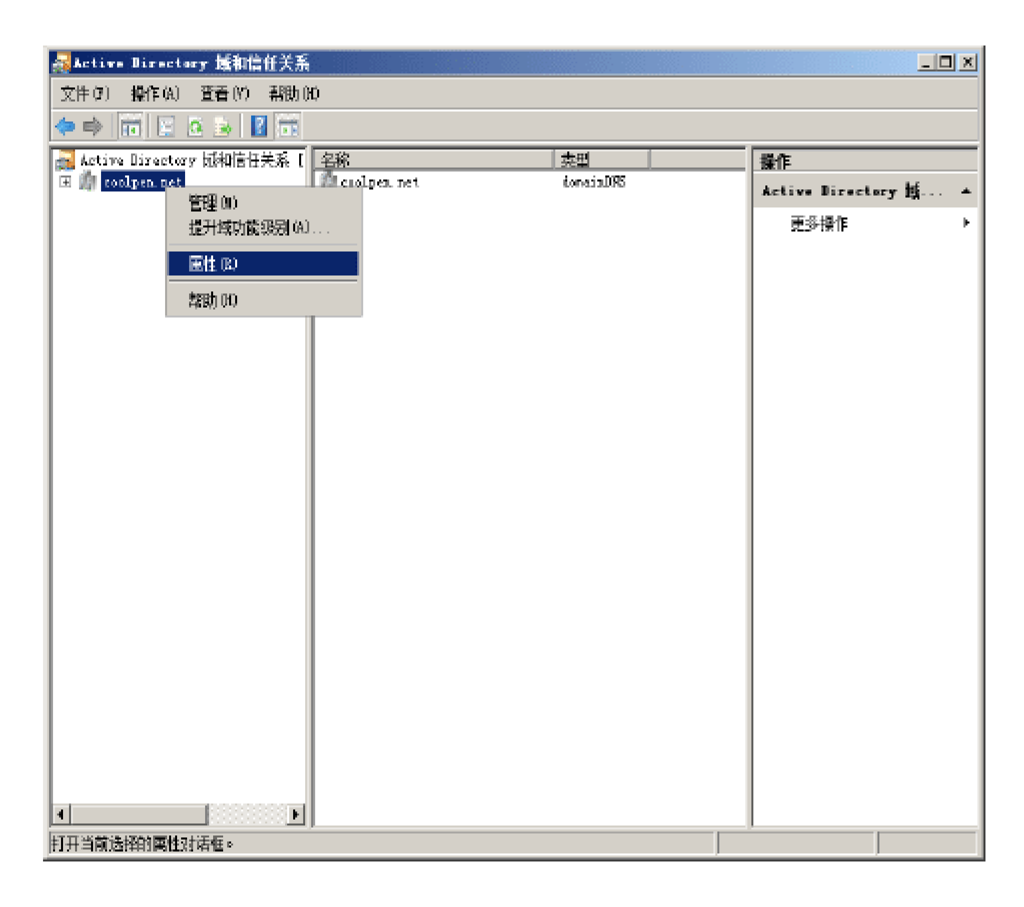


图 4.10　“Active Directory 域和信任关系”窗口

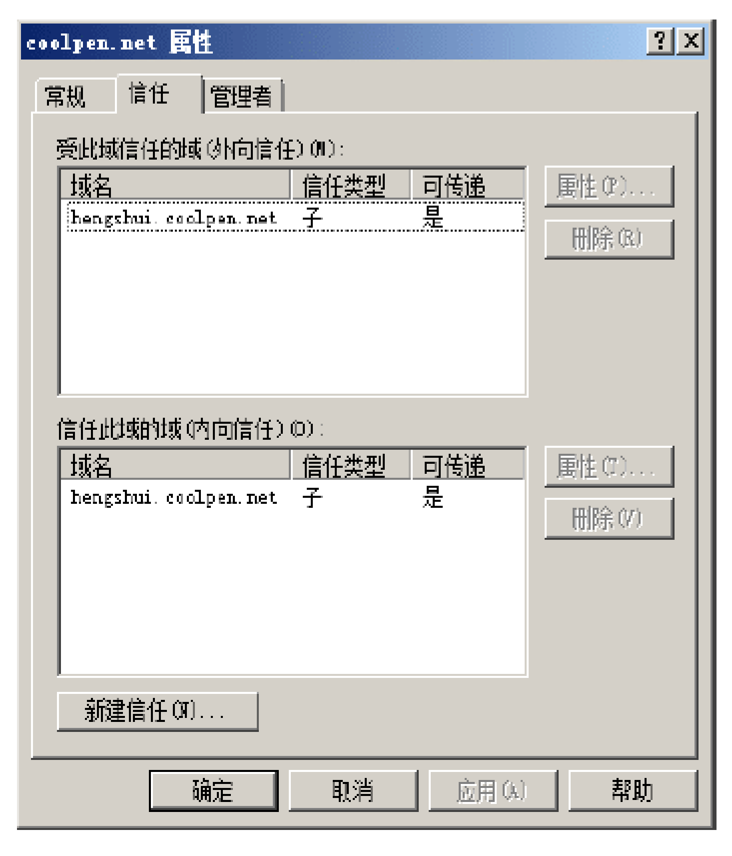


图 4.11　“信任”选项卡

03 单击“新建信任”按钮，启动“新建信任关系向导”，依次单击“下一步”按钮，设置信任名称和信任方向，如图 4.12 所示。信任名称可以使对方域控制器的 NetBIOS 或 DNS 名称。

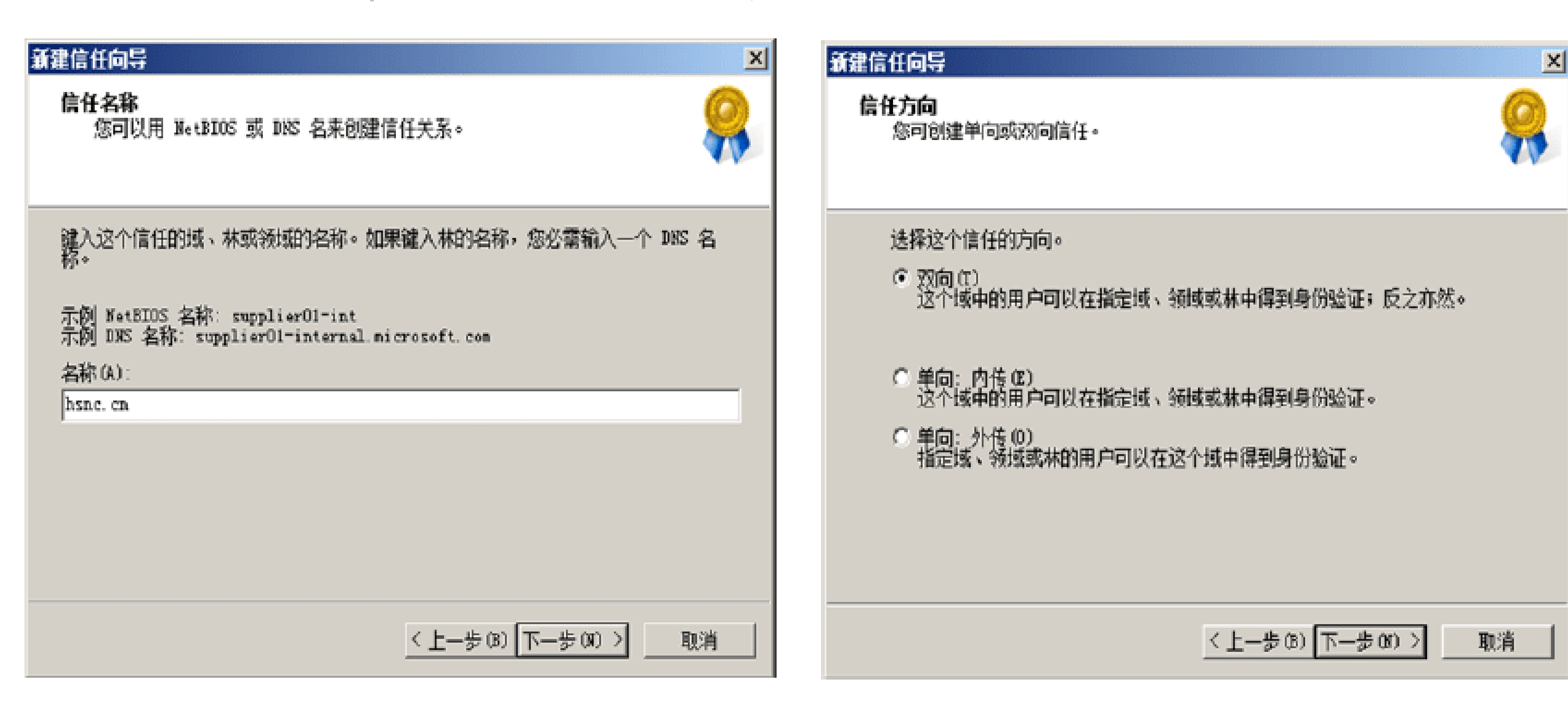


图 4.12 设置信任名称和方向

04 依次单击“下一步”按钮，选择信任方和设置信任密码，如图 4.13 所示。如果管理员具有每个域的管理员权限，可以通过选择“此域和指定的域”单选按钮，同时创建双方外部信任，否则选择“只是这个域”单选按钮，有对方域控制器的管理员完成相应操作即可。

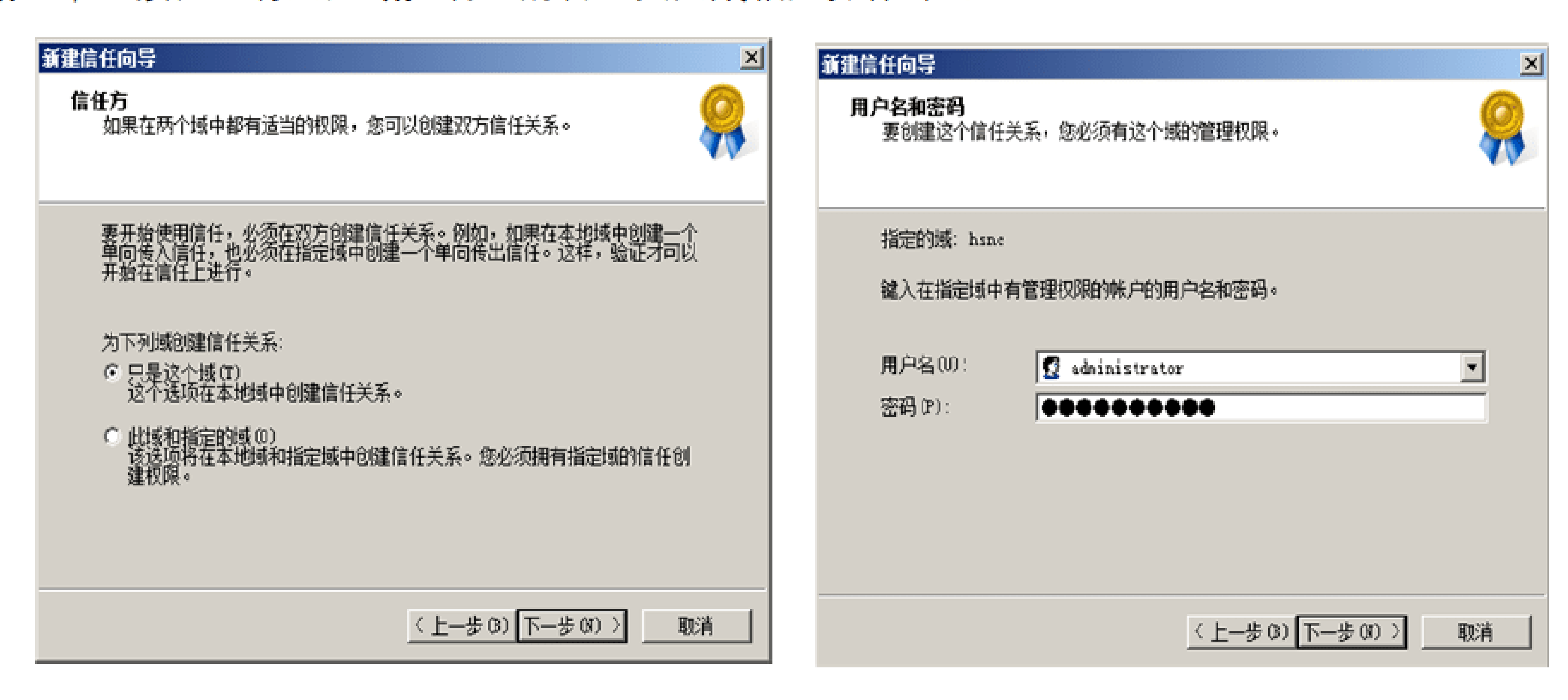
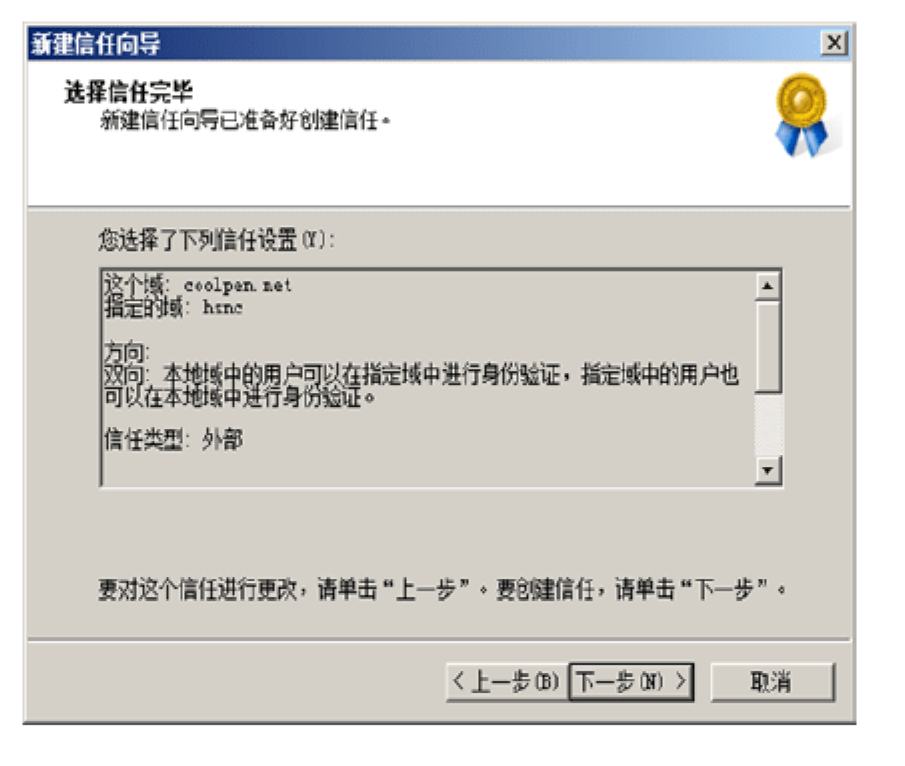


图 4.13 选择信任方并设置密码

05 依次单击“下一步”按钮，显示设置摘要并开始创建信任关系，直至创建信任关系完毕，如图 4.14 所示。创建完毕后，还可继续对该信任关系的某些选项进行配置，根据创建过程中选择选项的不同，配置选项也会有所不同。



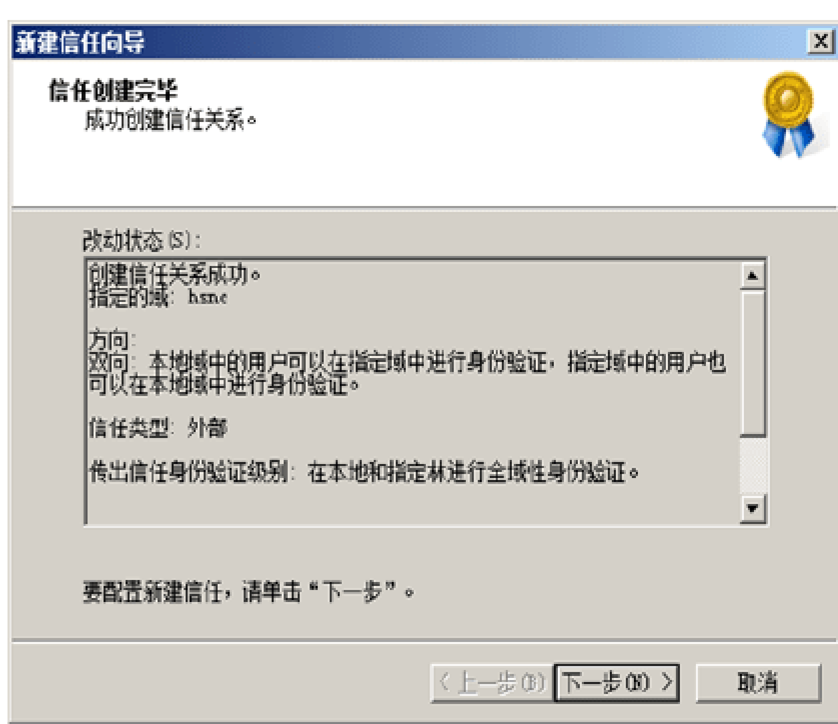


图 4.14 信任创建完毕

06 依次单击“下一步”按钮，确认当前信任关系的传出和传入类型，如图 4.15 所示。如果在“信任方”对话框中，选择了“只有这个域”单选按钮，即只在当前域控制器上创建信任关系操作，则此处应选择“否，不要确认传出信任”单选按钮，“确认传入信任”对话框的设置同样如此。

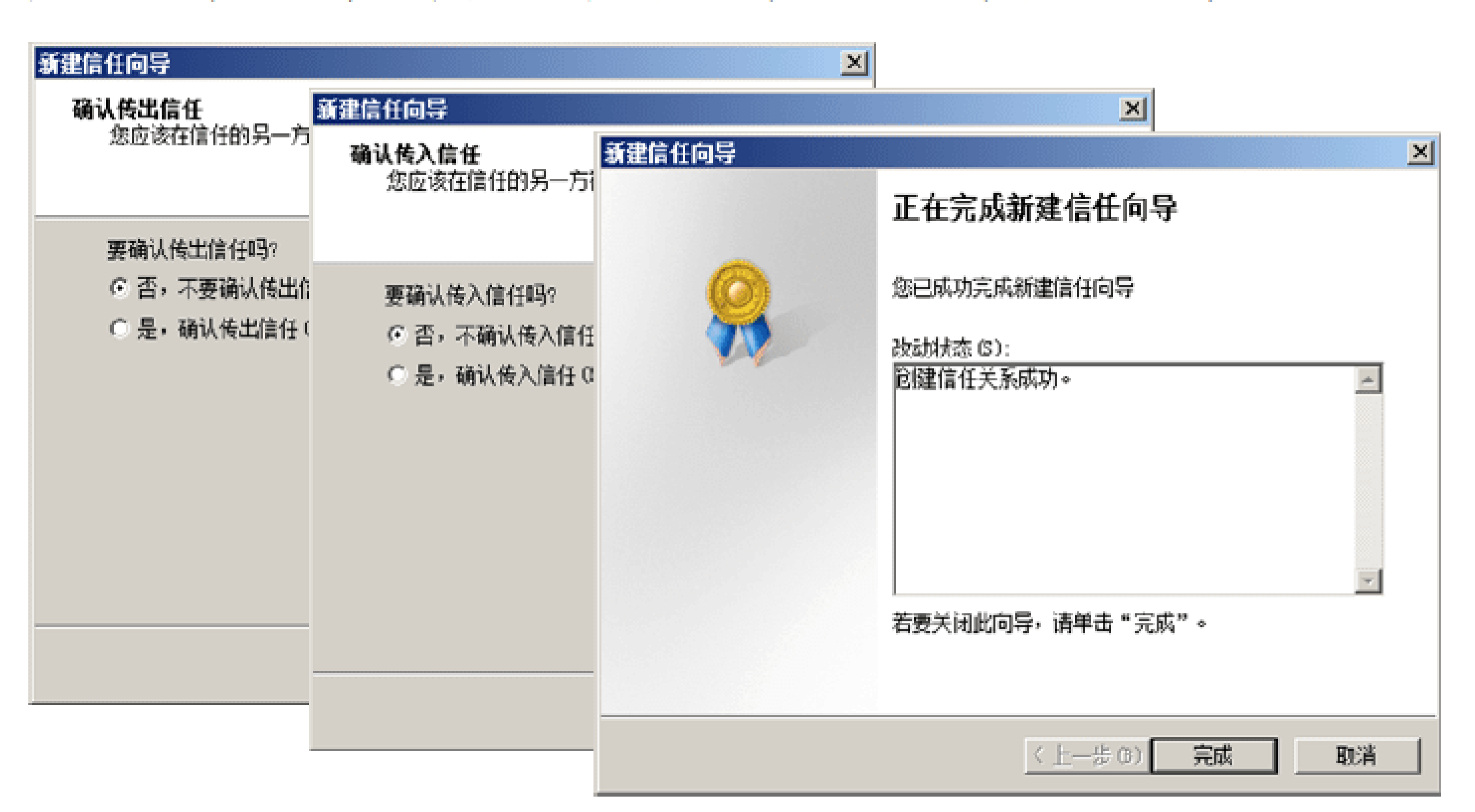


图 4.15 是否确认传出和传入信任



提示 如果创建信任关系过程中选择的是“单向：传出”或者“单向：传入”信任方式，则配置过程中就不会同时出现“确认传入信任”和“确认传出信任”对话框。

07 单击“完成”按钮关闭新建信任向导，打开如图 4.16 所示“Active Directory 域服务”对话框，提示已经启用 SID（安全识别符）筛选功能。SID 筛选用于防止可能试图将提升的用户权限，授予其他用户帐户的恶意用户攻击。强制 SID 筛选不会阻止同一林中的域迁移使用 SID 历史记录，而且也不会影响全局组的访问控制策略。对外部信任关系而言，SID 筛选功能会影响以下两个区域中现有 Active Directory 基础结构：

- 将会从受信域发出的身份验证请求中删除 SID 历史数据，这些 SID 历史数据包含除该受信域外的所有域中的 SID。这会导致拒绝访问具有用户旧 SID 的资源；
- 林间通用组访问控制的策略将需要更改。

08 单击“确定”按钮，返回“coolpen.net 属性”对话框，新创建的信任关系已经显示在列表中，如图 4.17 所示。

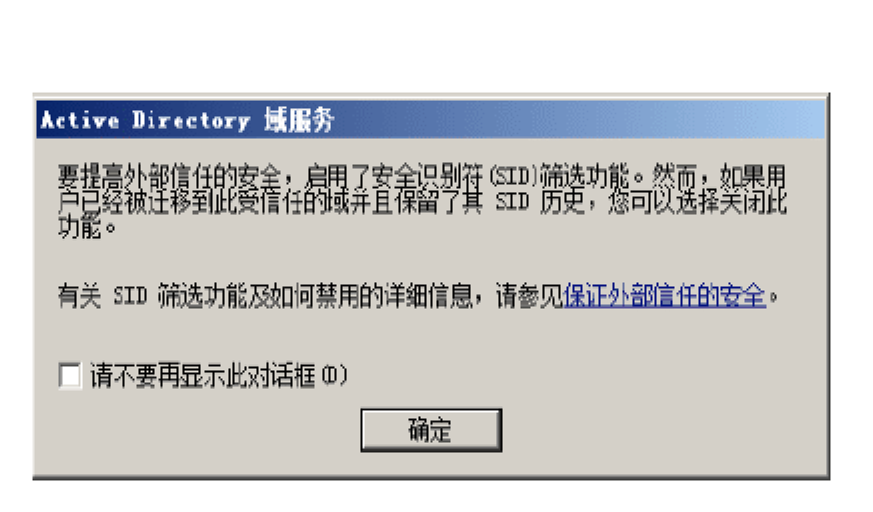


图 4.16 “Active Directory 域服务”对话框

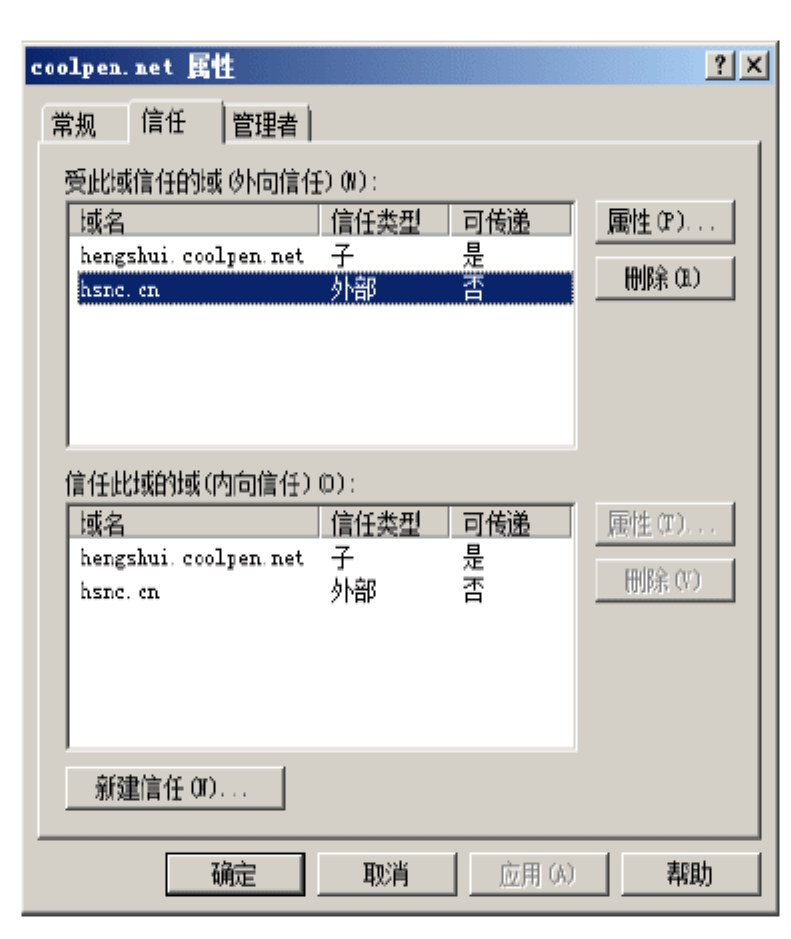


图 4.17 创建成功的信任关系

在另一台域控制器（本例中的 hsnc.cn）上，执行如下操作：

01 打开“Active Directory 域和信任关系”窗口，右击域名 hsnc.cn，选择快捷菜单中的“属性”选项，打开“hsnc.cn 属性”对话框，切换至如图 4.18 所示“信任”选项卡，默认已经显示了刚刚创建的信任关系。

> 提示 如果创建的是单向信任关系，则已创建的信任关系只会出现在“受此域信任的域（外向信任）”或“此域信任的域（内向信任）”中的一个列表框中，但确认创建信任关系的操作步骤与双向信任完全相同。

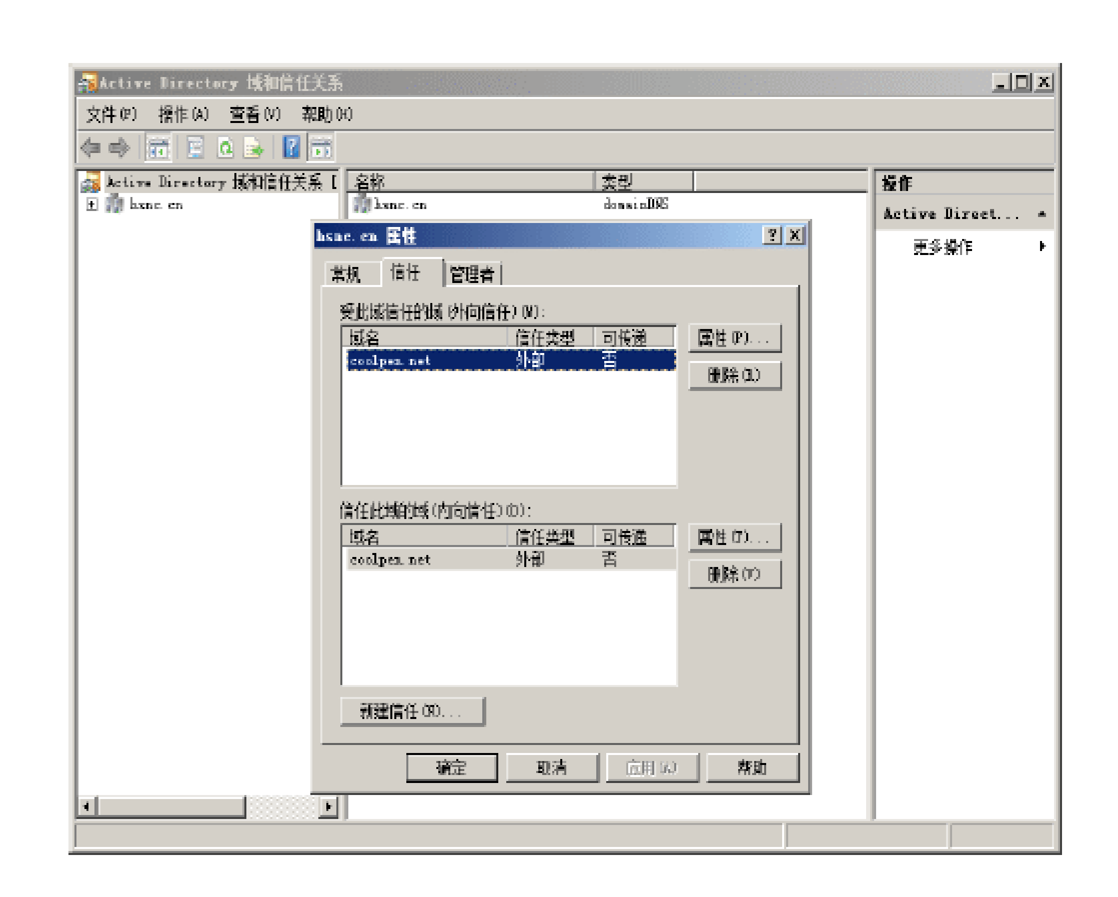


图 4.18 显示 hsnc.cn 属性

02 在“受此域信任的域（外向信任）”列表框中，选择“coolpen.net”并单击“属性”按钮，打开“coolpen.net 属性”对话框。单击“验证”按钮，显示“Active Directory 域服务”对话框，验证信任传入方向时，必须有对方域控制器的管理员权限。选择“是，验证传入信任”单选按钮，并在“用户名”和“密码”文本框中，分别输入域控制器 coolpen.net 上的管理员帐户名称和密码。如图 4.19 所示。

03 单击“确定”按钮，完成传入信任验证之后，还需要在“此域信任的域（内向信任）”选项框中，单击“属性”按钮，执行同样操作，以完成传出信任的验证。

04 在域属性对话框的“身份验证”选项卡中，还可以对用户在各个域上执行的身份验证方式进行选择，在如图 4.20 所示“coolpen.net 属性”对话框中，可以为来自 coolpen.net 域的用户帐户选择身份验证范围。



图 4.19 设置 coolpen.net 属性

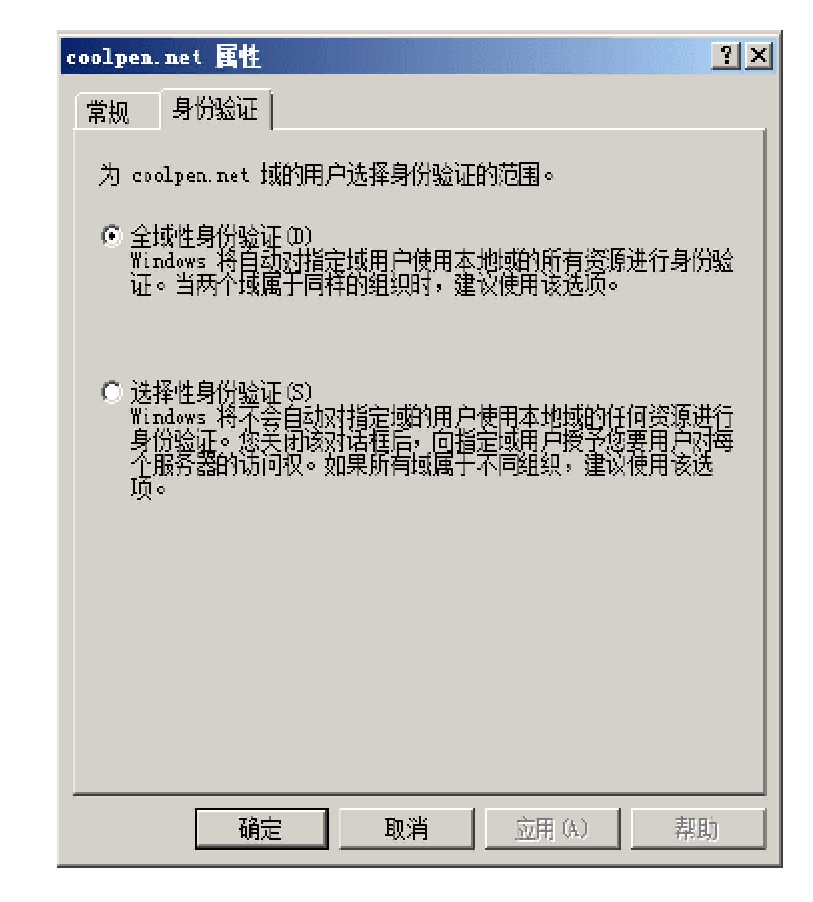


图 4.20 “身份验证”选项卡

包括如下两种身份验证方式：

- 全域性身份验证：域控制器 coolpen.net 上的用户使用域控制器 hsnc.cn 上的资源时，需要通过两台域控制器上设置的所有身份验证方式；
- 选择性身份验证：域控制器 hsnc.cn 将不会对来自域控制器 coolpen.net 的用户访问进行



任何身份验证，对 hsnc.cn 下属子域同样具有不受身份验证的“特权”。

至此两台域控制器之间即可成功建立信任关系，这两个域的用户即可以自由访问另外一个域的信息（如果选择单向信任则另当别论）。如图 4.21 所示，是一台加入域控制器 coolpen.net 主机名为 coolpen-c8 的计算机的登录窗口，在“登录到”下拉列表中显示了本地计算机、域控制器 coolpen.net 以及其所有信任的域，用户可根据需要选择登录到的对象。



图 4.21　“登录到 Windows”窗口

4.4　权限委派

在 Windows Server 2008 网络中，可将单个组织单位和独立域的管理权限彻底委派给用户，这样可减少需要具有较高管理权限的管理员用户帐户。通过委派，让信任用户可以在一个特定容器内改变属性、创建或删除某种类型的对象以及更改某种类型对象的某些属性等。

4.4.1　权限委派概述

通过在域中创建组织单位并将特定组织单位的管理控制权，委派给特定用户或组，可将管理控制权委派给域树的任何层次。例如，可以创建一个组织单位，该组织单位允许将某个部门（如“图书馆”）的所有分支中，所有用户和计算机帐户的管理控制权指派给用户。也可以只把部门内的某些资源（例如计算机帐户）的管理控制权指派给用户。另一种可能的管理控制委派是将“图书馆”组织单位（而不是“图书馆”组织单位内包含的任何组织单位）的管理控制权指派给用户。

Active Directory 定义了特定的权限和用户权利，可用于委派或限制管理控制权。通过使用组织单位、组和权限的组合，可以定义某个人最适合管理范围，可以是整个域、域内的所有组织单位，或单个组织单位。

使用“控制委派向导”或通过“授权管理器”控制台，可以将管理控制权指派给用户或组。这两种工具都允许给特定用户或组指派权利或权限。例如，可以为用户授予修改“帐户所有者”属性的权限，而不指派删除该组织单位中的帐户权限。正如其名称所示，“控制委派向导”允

许使用向导委派管理任务，该向导将带领用户逐步经过整个过程。“授权管理器”是一个也允许委派管理的 Microsoft 管理控制台。“授权管理器”比“控制委派向导”提供了更大的灵活性，但更加复杂。

4.4.2 委派操作权限

默认情况下，在 Windows Server 2008 域中，可以使用如下两种方式，将普通权限（以在“阅览室”OU 中“创建子对象”权限为例）委派给指定的用户帐户或组（以“liuxh”帐户为例）。一是直接在高级选项模式下，将权限委派给指定的全局安全组或组中的对象；二是在任意模式下，借助委派控制向导，将操作权限委派给指定对象。

1. 高级功能模式权限委派

默认情况下，“Active Directory 用户和计算机”窗口中显示的只是对象的普通属性设置，但委派权限需要修改对象的“安全”属性，必须切换到“高级”功能模式下执行。另外，需要委派的操作权限，也可以分为普通权限和特殊权限两种，操作方法略有不同。

（1）普通权限

“普通权限”只是一些常用权限，如读取、写入、完全控制等。

01 以管理员帐户登录域控制器，在“Active Directory 用户和计算机”窗口中，单击“查看”菜单中的“高级功能”选项，如图 4.22 所示。

02 右击“阅览室”组织单位，选择快捷菜单中的“属性”选项，打开“阅览室 属性”对话框，切换到如图 4.23 所示“安全”选项卡。要承担委派权限的用户帐户 liuxh 默认并没有显示在“组或用户名”列表中。单击“添加”按钮，打开“选择用户、计算机或组”对话框，在“输入对象名称来选择”文本框中，输入用户帐户名 liuxh 并单击“检查名称”按钮，验证是否正确。

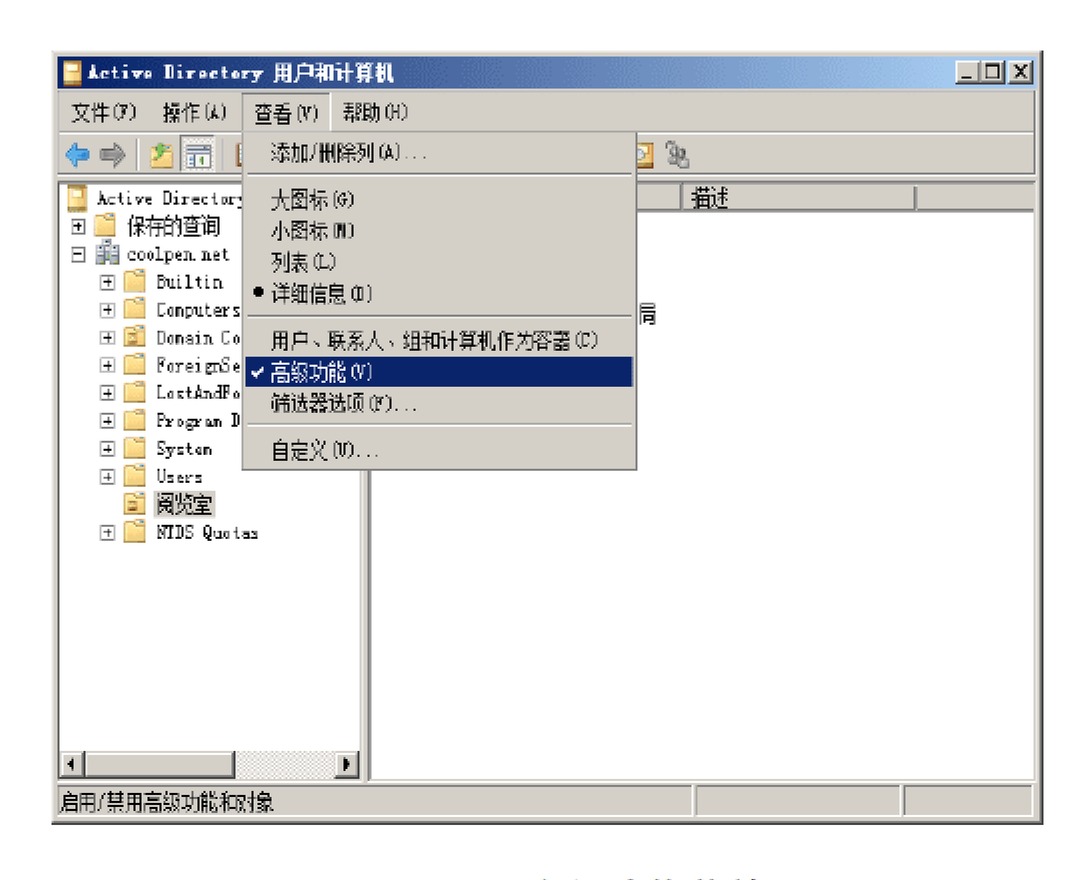



图 4.22 高级功能菜单项



图 4.23 添加被委派操作权限的用户帐户

03 单击“确定”按钮，将其添加到“组或用户名”列表中，选中“liuxh”帐户名，并在对应的“liuxh 的权限”列表中，选中“创建所有子对象”权限的“允许”复选框，如图 4.24 所示。系统默认只赋予用

户“读取”权限，此处可以保留该权限，也可以删除。

04 单击“确定”按钮，保存设置。

为了验证委派权限是否生效，可以在网络中任意工作站上，以 liuxh 帐户登录到域，并通过控制台，远程连接到域控制器，打开“Active Directory 用户和计算机”窗口。在“阅览室”组织单位上，单击鼠标右键，会发现快捷菜单中的“新建”选项，如图 4.25 所示。默认情况下，普通用户帐户在其他任何组织单位或容器上，都不会拥有该权限，即快捷菜单中不会出现“新建”选项。



图 4.24　赋予用户权限

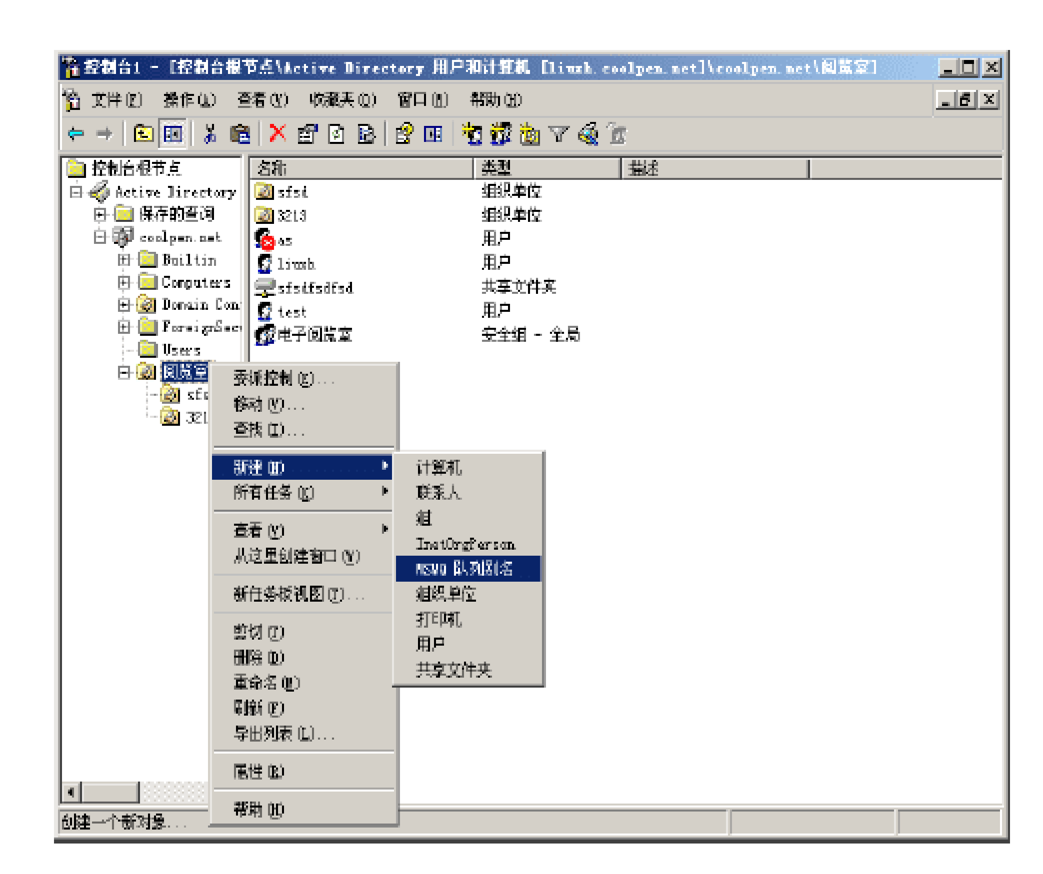


图 4.25　用户行使被委派的权限



注意　用于远程连接域控制器管理控制台的计算机，必须已安装 Active Directory 服务，否则无法添加“Active Directory 用户和计算机”管理单元。

委派的权限只能作用于目标对象，即不会自动传播到其所包含的子对象上。在本例中，liuxh 帐户只能在“阅览室”组织单位中创建子对象，如 OU、用户、组等，但无法在这些子 OU 或组中继续创建对象。

（2）特殊权限

“特殊权限”是针对“普通权限”而言的，不仅权限种类多于普通权限，更重要的是，权限划分更加详细，管理员可以通过它进行更为准确的权限委派，确保网络安全。仍以“阅览室”组织单位和 liuxh 帐户为例，不同的是，只赋予用户帐户在该 OU 中创建用户“帐户”的权限，而不允许创建其他类型子对象。

01 打开“阅览室 属性”对话框的“安全”选项卡，单击“高级”按钮，显示如图 4.26 所示“阅览室 的高级安全设置”对话框，在这里可以查看当前作用于该对象的所有权限项目。

02 在“权限项目”列表中选中 liuxh 帐户对应的项目，单击“编辑”按钮，显示如图 4.27 所示“阅览室 的权限项目”对话框。取消“创建所有子对象”权限的“允许”复选框，仅保留“创建 用户 对象”即可




图 4.26 “阅览室 的高级安全设置”对话框

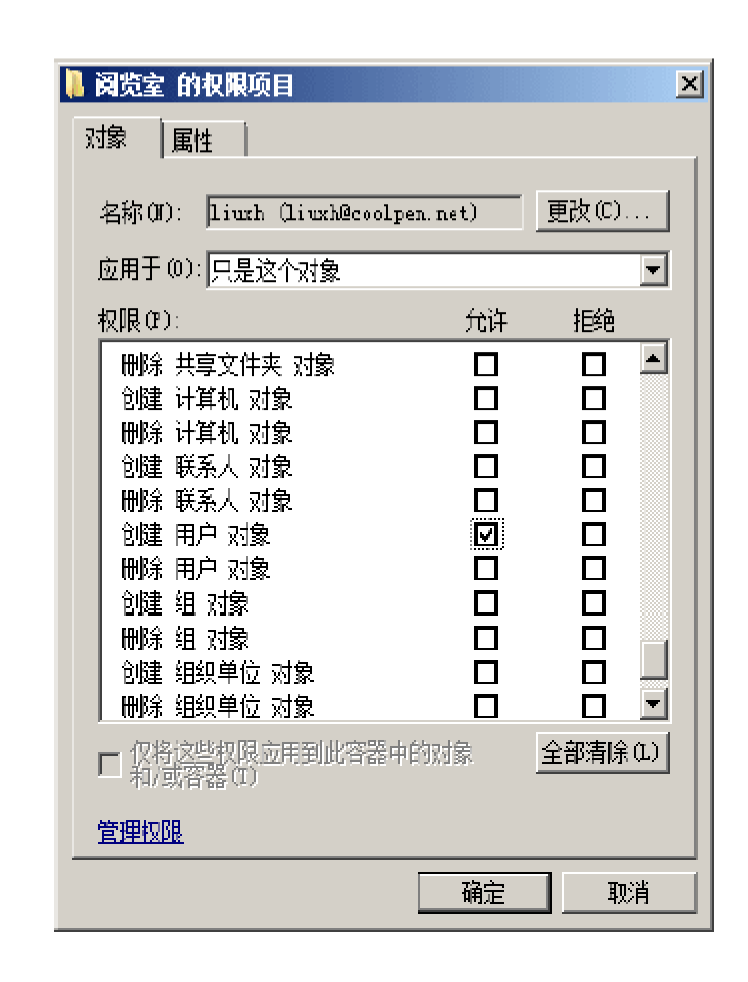


图 4.27 “阅览室 的权限项目”对话框

03 单击“确定”按钮，保存设置。

此时，再次测试 liuxh 帐户被委派的操作权限，即可发现“新建”选项中只包括“用户”对象类型了，如图 4.28 所示。

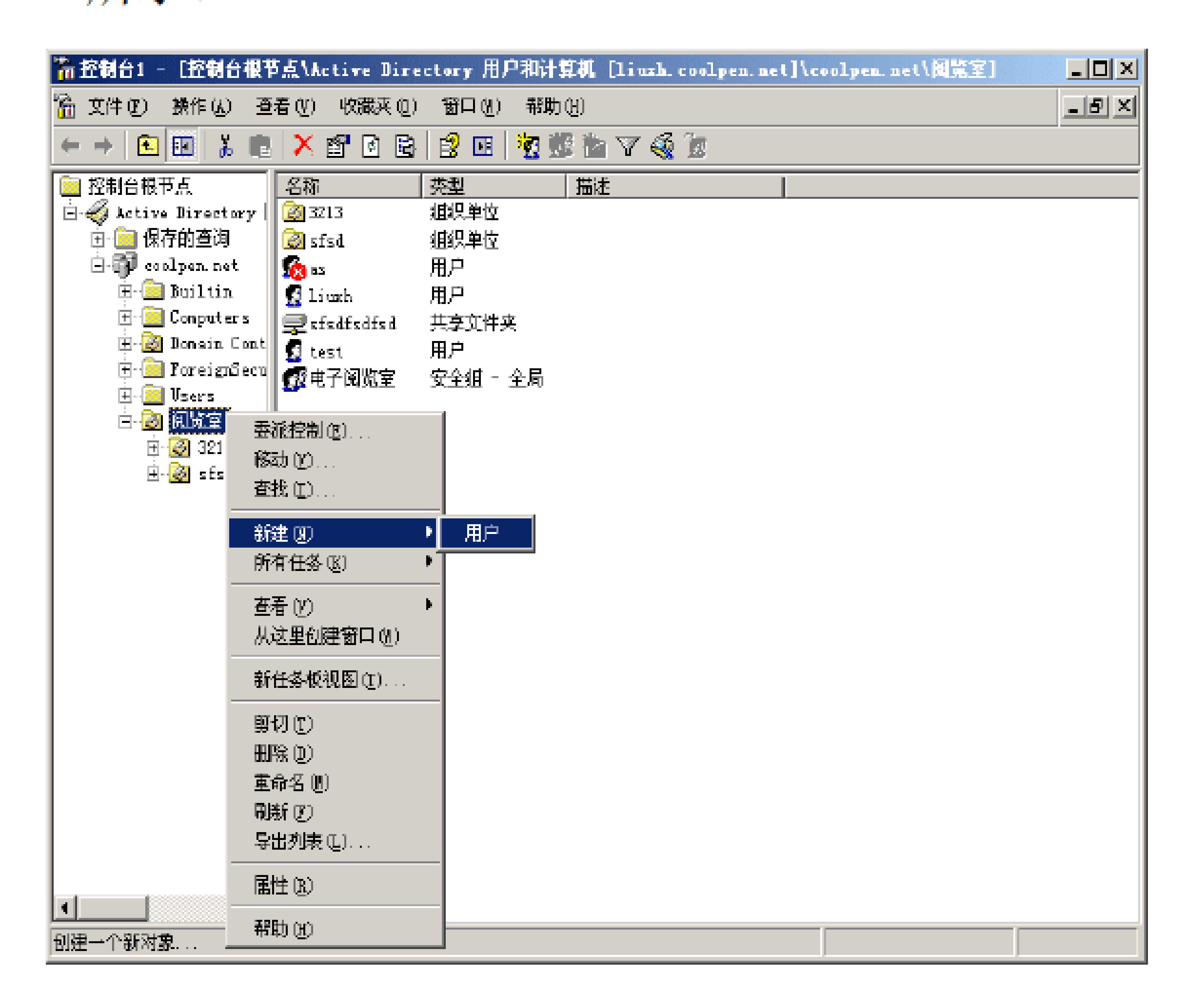


图 4.28 被委派的特殊权限

2. 委派控制向导

与上述方式相比，委派控制向导方式更为简单，无须更改显示模式，即可将操作权限准确指派给用户帐户或组。

01 打开“Active Directory 用户和计算机”窗口，右击“阅览室”并选择快捷菜单中的“委派控制”选项，启动控制委派向导。单击“下一步”按钮，显示如图 4.29 所示“用户和组”对话框。在这里需要将用于承担委派权限的用户帐户添加到“选定的用户或组”列表中。



图 4.29　选择用户和组

02 单击“下一步”按钮，显示如图 4.30 所示“要委派的任务”对话框。在“委派下列常见任务”列表中，选中“创建、删除和管理用户帐户”和“创建、删除和管理组”复选框。

03 单击“下一步”按钮，显示“完成控制委派向导”对话框，并显示了前面所设置的信息，如图 4.31 所示。

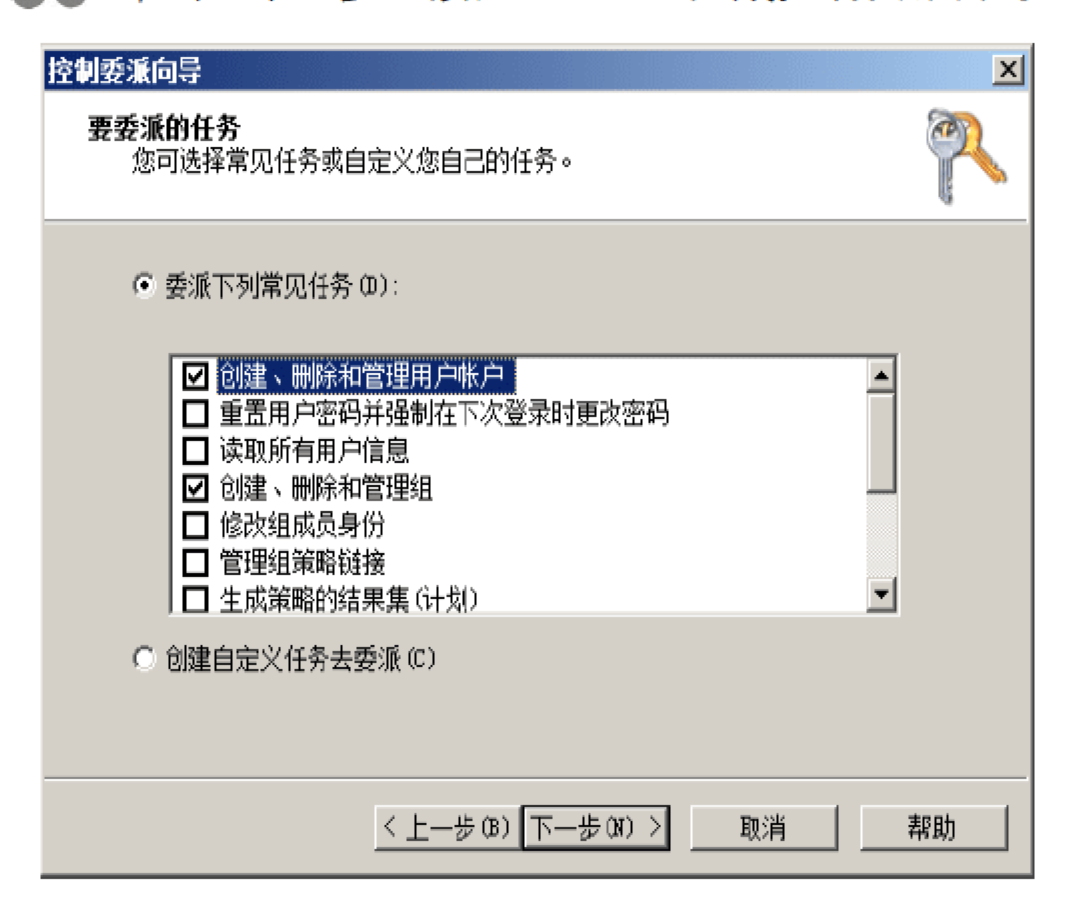


图 4.30　“要委派的任务”对话框



图 4.31　“完成控制委派向导”对话框

04 单击“完成”，即可完成委派任务操作。

4.4.3　RODC 的部署与应用

在 Windows Server 2008 系统中，管理员既可以通过 AD DS 安装向导安装，也可以使用 dcpromo /adv 的命令行安装。使用向导模式更加直观，适用于初级用户。推荐使用 AD DS 安装向导的高级安装模式，在高级模式下用户可以设置更多选项。

1. RODC 部署要求

如果需要部署 RODC，在网络中必须有一台安装或者升级到的 Windows Server 2008 的域控制器。部署之前，管理员应注意以下事项：

■ Active Directory 数据库复制。RODC 支持从 Windows Sever 2008 域控制器复制架构分区和配置分区的数据，但是 RODC 只能从来自同一域的 Windows Server 2008 的可读写域控制器复制域分区的数据更新。因此，在网络中至少安装一台 Windows Server 2008 的域控制器用于 RODC 复制；
■ 林功能级别。部署 RODC 需要森林的功能级别最低为 Windows Server 2003 模式，建议使用 Windows Server 2008 模式。用户可以通过在“Active Directory 域和信任关系”窗口中，提升到所需的林功能级别；
■ Windows Server 2008 域控制器的角色为主域控制器，否则将无法识别 RODC 使用的特殊的 Kerberos 票据授权票（KRBTGT）帐户；
■ RODC 默认不缓存帐户，必须在可读写域控制器上启用帐户缓存功能后，才可以用于缓存域用户帐户；
■ RODC 安装完成后，默认连接的是当前所有的可读写域控制器，必须在 RODC 上，通过“更改域控制器”使其连接到已部署的 RODC 上。

2. 添加缓存帐户

在主域控制器中，设置可以在 RODC 上缓存的用户分支机构。建议为分支机构创建单独的组织单位，在该组织单位下创建组，组的创建规则建议符合企业的行政管理架构，以降低管理的复杂度。默认情况下，RODC 并未保存所有域用户帐户的信息，可以按照如下方法，将需要缓存的用户帐户，添加到 RODC 的缓存策略中。

01 在 RODC 上，依次选择“开始”→“管理工具”→“Active Directory 用户和计算机”选项，打开如图 4.32 所示“Active Directory 用户和计算机”窗口，此时连接到的域控制器状态为“只读”。

02 依次选择“coolpen.net”→“Domain Controllers”选项，双击“LIUXH-RODC”显示“LIUXH-RODC 属性”对话框，切换到如图 4.33 所示“密码复制策略”选项卡。

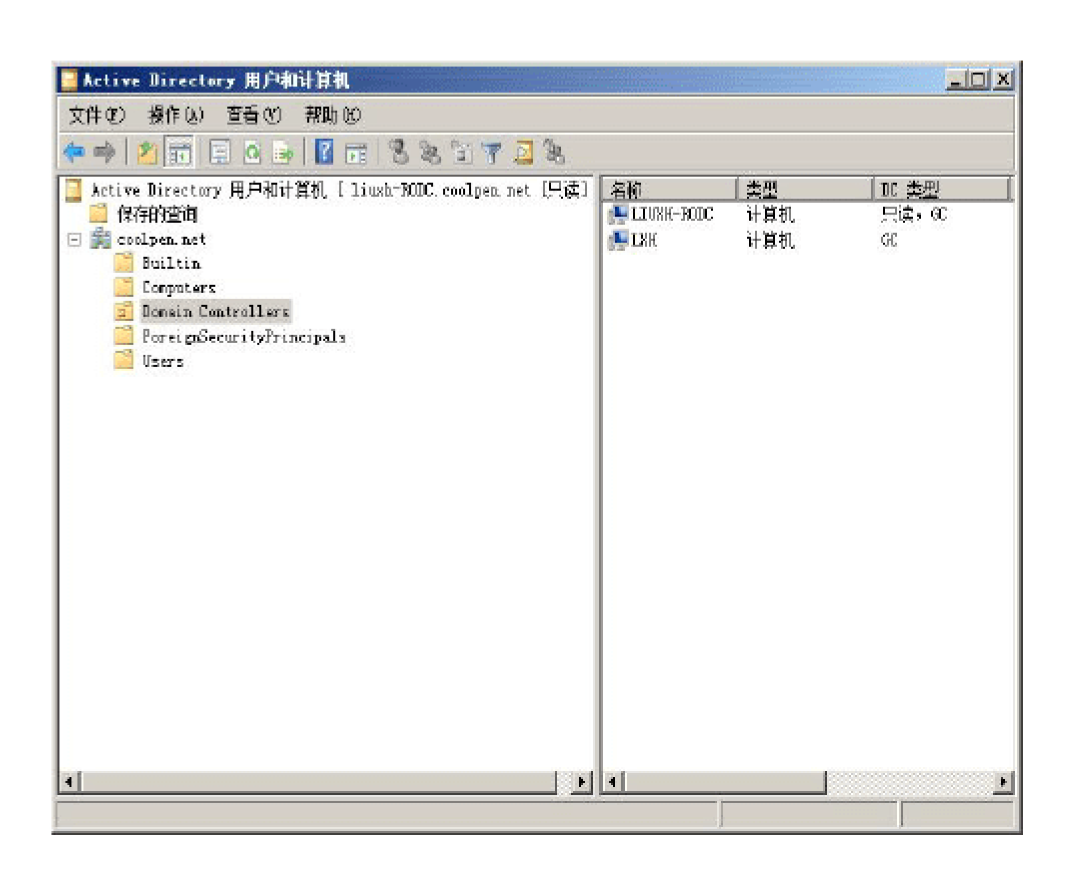


图 4.32 “Active Directory 用户和计算机”窗口

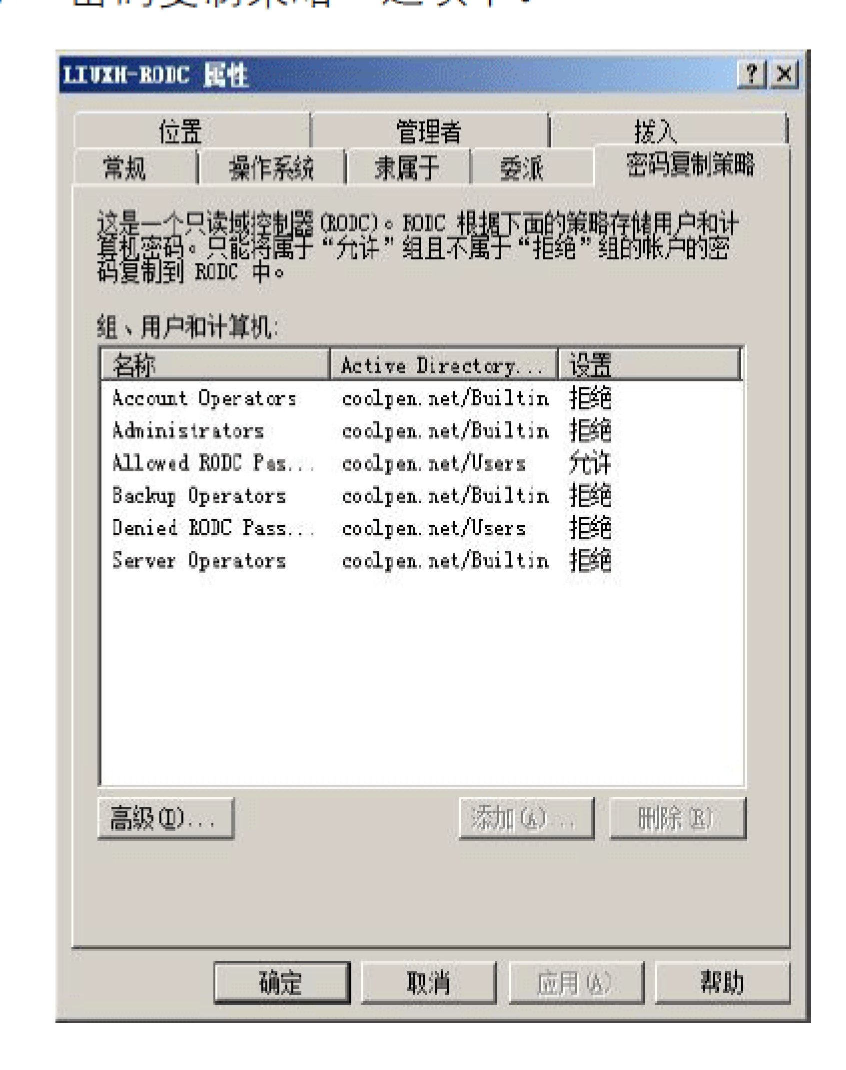
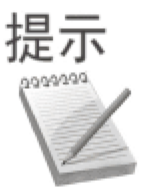


图 4.33 “密码复制策略”选项卡



提示 单击“高级”按钮，显示如图 4.34 所示“以下项目的高级密码复制策略 LIUXH-RODC”对话框，这里显示的是密码复制策略的高级功能，用户可以根据

需要选用。在“策略使用率”选项卡的“显示满足下列条件的用户和计算机”下拉列表中，包括如下选项：

- 选择“其密码已经存储在只读域控制器中的帐户”选项，除了 RODC 自身的计算机帐户和 Kerberos 票据授权 (KRBTGT)帐户之外，默认情况下没有缓存任何帐户的密码。
- 选择“已通过此只读域控制器身份验证的帐户”选项，显示在 RODC 进行身份验证的用户以及计算机，通过此列表确定允许哪些帐户的密码，在此 RODC 域控制器中进行缓存。

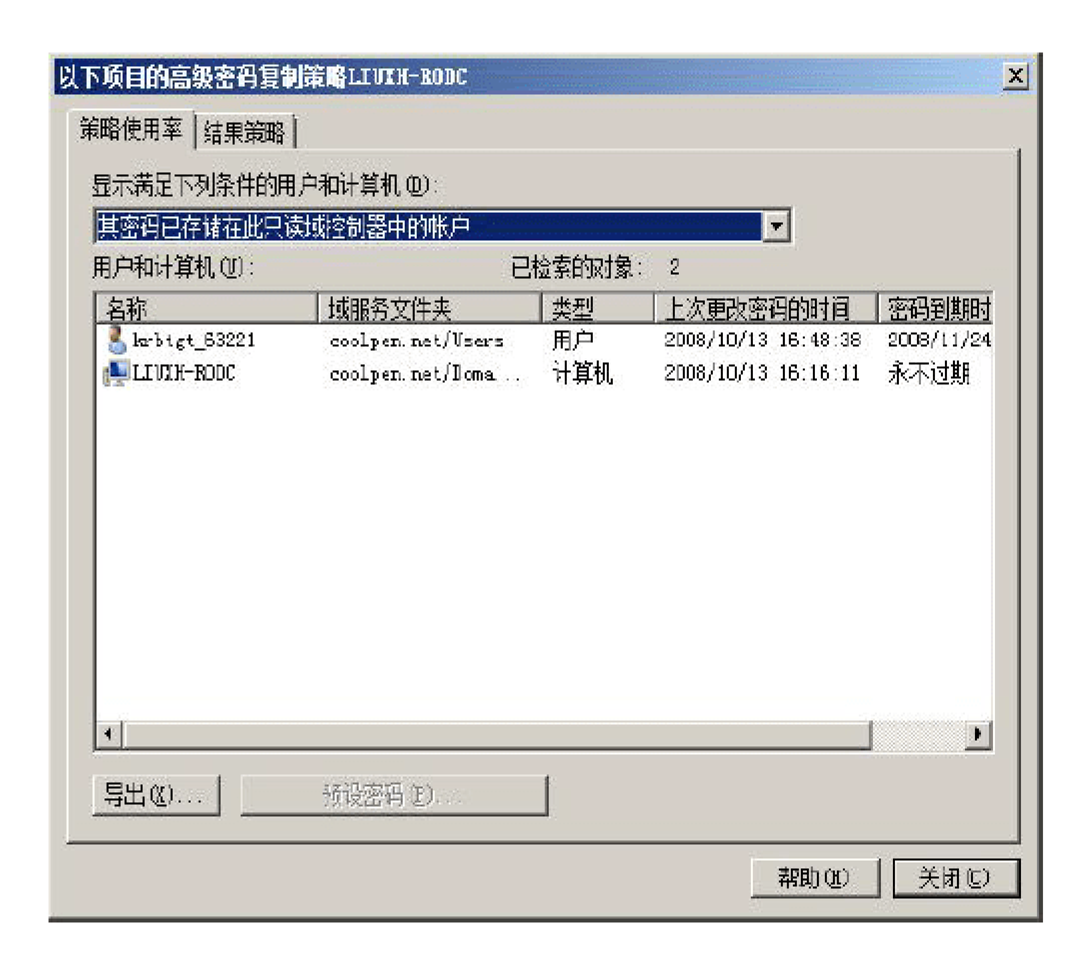


图 4.34　“以下项目的高级密码复制策略 LIUXH-RODC”对话框

03 单击“添加”按钮，显示如图 4.35 所示“添加组、用户和计算机”对话框。设置 RODC 域控制器中允许或者拒绝缓存的组、用户和计算机，这里选择“允许该帐户的密码复制到此 RODC 中”单选按钮。

04 单击“确定”按钮，显示如图 4.36 所示“选择用户、计算机或组”对话框，在“输入对象名称来选择”文本框中，输入想要添加的域用户帐户。

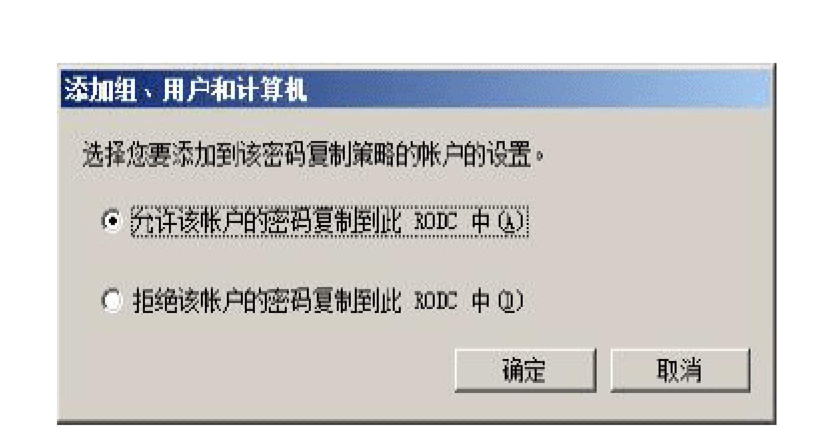




图 4.35　“添加组、用户和计算机”对话框　　图 4.36　“选择用户、计算机和组”对话框

05 单击“确定”按钮，关闭“选择用户、计算机或组”对话框，返回到“LIUXH-RODC 属性”对话框，如图 4.37 所示，所选用户帐户已被添加到列表中。

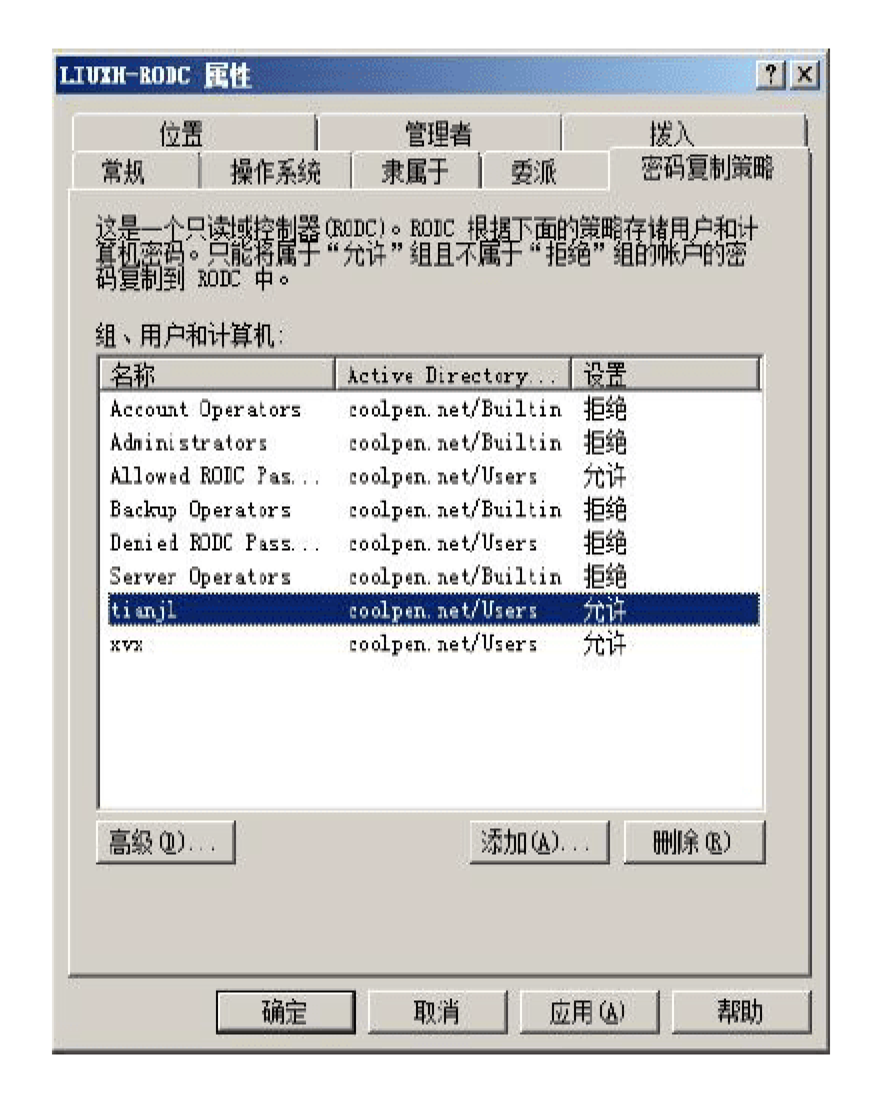


图 4.37 “LIUXH-RODC 属性”对话框

06 单击“应用”按钮，设置生效。

4.5 活动目录的备份与恢复

Active Directory 数据库是一个事务处理数据库系统。如果活动目录崩溃，对网络最直接的影响是网络用户不能直接登录，需要使用域用户方式验证访问的应用系统服务则不能进行数据访问，CA 证书不能认证等。因此，网络管理员需要定期备份活动目录数据库，当活动目录数据库出现问题时，可以通过备份的数据还原活动目录数据库。

4.5.1 安装 Windows Server Backup

Windows Server 2008 中没有提供类似 Windows Server 2003 或 Windows XP 的“备份和还原向导”，取而代之的是一个叫作“Windows Server Backup”的备份工具，该工具默认是不被安装的，需要在“服务器管理器”中手动添加。

打开“服务器管理器”窗口，展开“功能”，单击窗口右侧的“添加功能”超级链接，打开“添加功能向导”，在“选择功能”对话框中，选中“Windows Server Backup 功能”复选框。系统默认不会选择“命令行工具”，需要手动选择。依次单击“下一步”按钮，即可开始安装，如图 4.38 所示。

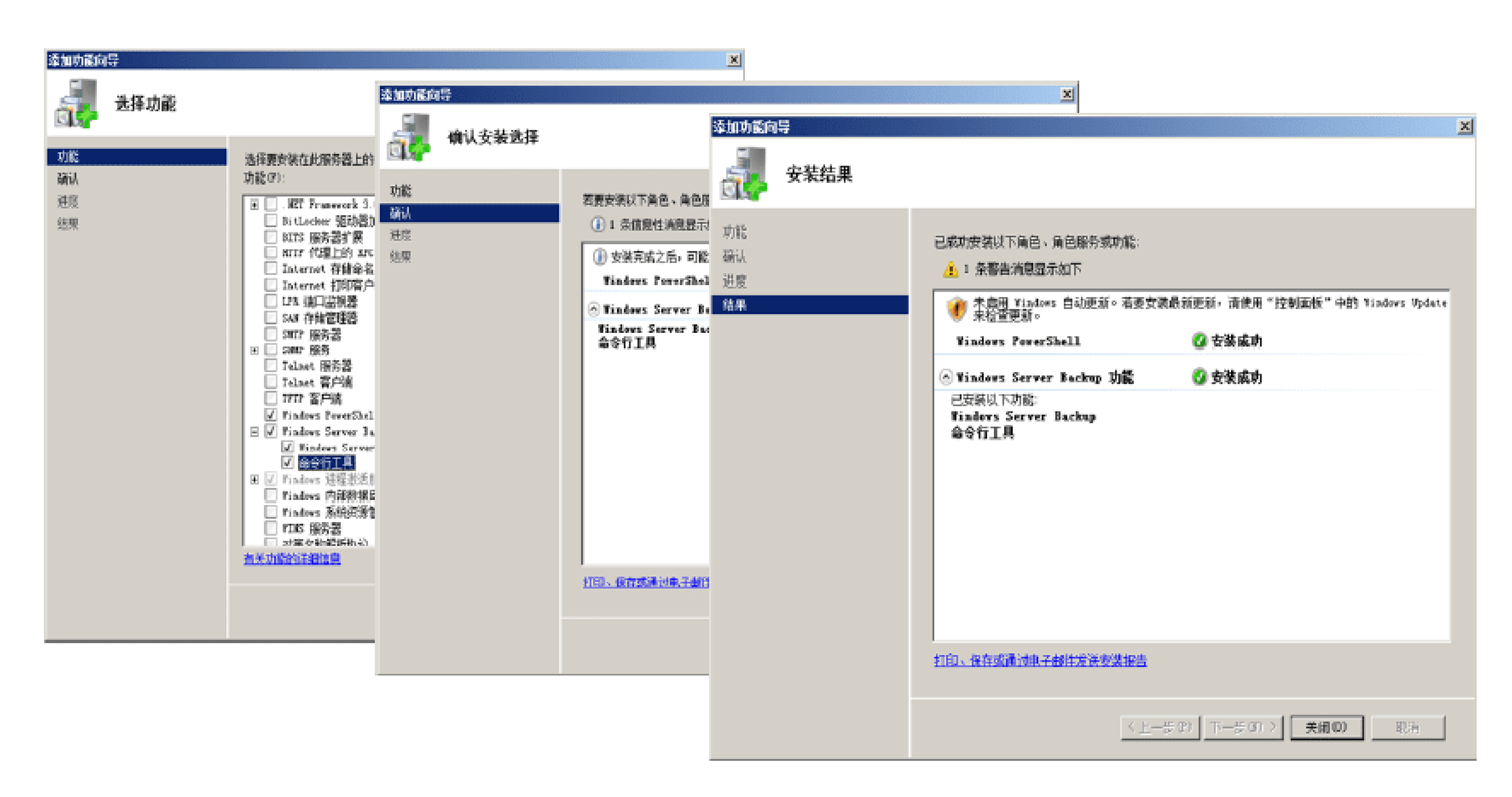


图 4.38　安装 Windows Server Backup

4.5.2　备份活动目录数据库

活动目录是一种实时性数据库，其中包含 Ntds.dit（活动目录数据库）、Edb.log（事件日志）、Temp.edb（记录数据库最后一个缓冲区的检查点文件和暂时性的数据库文件）等几个文件。事实上，目录服务是一个组合性系统，包括目录数据存储和用户或程序存取信息的相关服务。

01 单击“开始”→“命令提示符”选项，打开“命令提示符”窗口，输入如下命令：

Wbadmin get disks

回车执行，显示服务器已经联机的磁盘，如图 4.39 所示。其中，F 盘是将用来存储备份的磁盘。

```
管理员: 命令提示符
C:\Users\Administrator>wbadmin get disks
wbadmin 1.0 - 备份命令行工具
(C) 版权所有 2004 Microsoft Corp.

磁盘名称        : VMware, VMware Virtual S SCSI Disk Device
磁盘数量        : 0
磁盘标识符      : {b6cdbeeb-0000-0000-0000-000000000000}
总空间          : 41.00 GB
已用空间        : 8.77 GB
卷              : C:[(没有卷标签)],D:[(没有卷标签)]

磁盘名称        : VMware, VMware Virtual S SCSI Disk Device
磁盘数量        : 1
磁盘标识符      : {2ab5e863-0000-0000-0000-000000000000}
总空间          : 40.00 GB
已用空间        : 7.97 GB
卷              : F:[Backup]

C:\Users\Administrator>
```

图 4.39　已经联机的磁盘

02 在命令行提示符下键入如下命令：

wbadmin start systemstatebackup -backuptarget:f:

回车执行，显示询问是否要将系统状态从 C 盘备份到 F 盘，如图 4.40 所示。

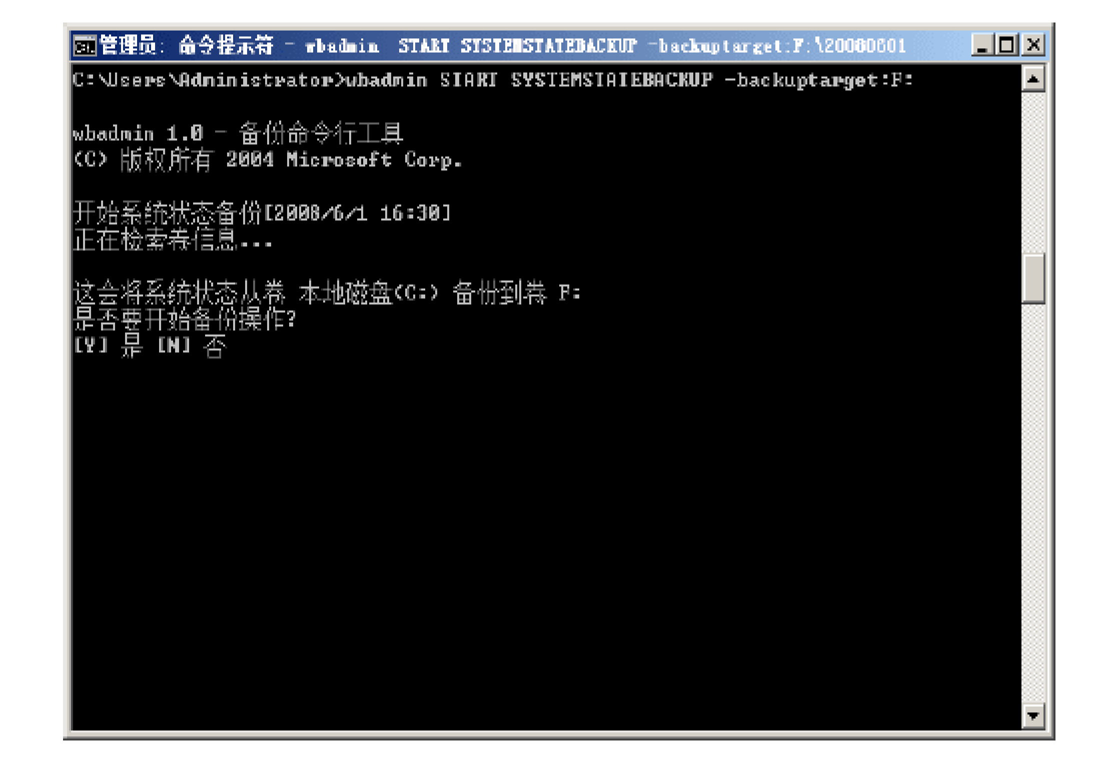


图 4.40　询问是否要将系统状态从 C 盘备份到 F 盘

03 按下键盘字母“Y”，按回车键创建需要备份的卷的卷影副本并搜索系统状态文件。搜索完成后，开始启动文件备份并显示备份进度。备份完成，并且创建了一个备份文件日志，如图 4.41 所示。

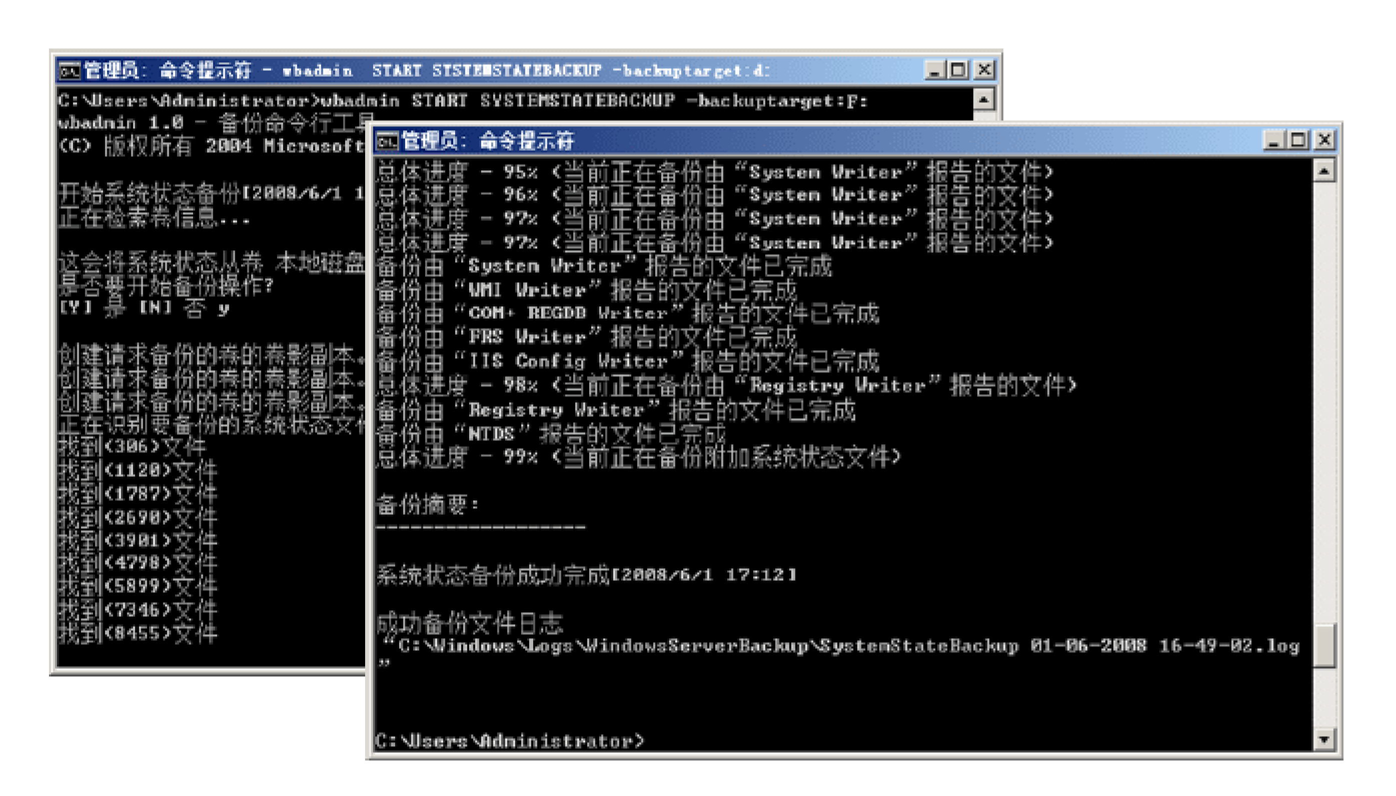


图 4.41　备份文件及日志

04 在命令行提示符下输入命令：wbadmin get versions

回车执行，显示备份信息，包括备份时间、备份目标及可以恢复的组件等。至此，活动目录备份完成。

4.5.3　恢复活动目录数据库

Windows Server Backup 采用了新的数据恢复机制，如果只是恢复文件及文件夹，可以使用恢复向导完成；如果恢复 Active Directory 数据库，则需要在目录还原模式下使用“Wbadmin.exe”命令完成。

01 重新启动系统，选择“目录还原模式”启动，并以系统管理员帐户登录到本地计算机。注意，此时域是不可用的，只能登录到本地系统。打开“命令提示符”窗口，输入命令：wbadmin get versions 回车执行，显示 Active Directory 服务器的备份列表及需要注意每次备份中的版本标识符，如图 4.42 所示。

02 在命令行提示符下，输入命令：WBADMIN START SYSTEMSTATERECOVERY -version: 06/01/2008-08:49 回车执行，命令成功执行，提示网络管理员是否要执行系统状态恢复操作。按下键盘字母“Y”，确认执行系统状态恢复，按回车键开始处理要还原的文件，如图 4.43 所示。文件处理完成后，开始从备份还原文件并显示还原进度。



图 4.42　备份列表

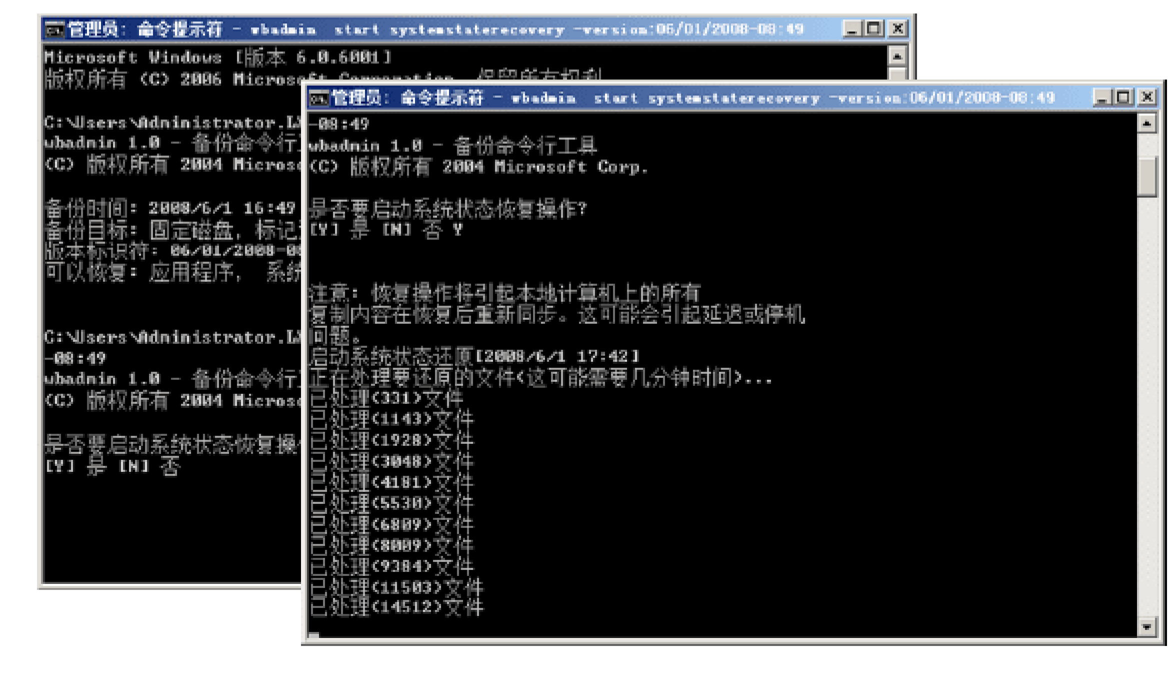


图 4.43　处理要还原的文件

03 系统状态还原完成，并创建了还原日志。同时提示需要重新启动计算机尝试恢复系统文件，如图 4.44 所示。

04 重新启动系统并登录，提示系统恢复操作已完成，如图 4.45 所示。按回车键，退出命令行工具即可。

```
管理员: 命令提示符
总体进度 - 96% (当前正在还原由 "System Writer" 报告的文件)
总体进度 - 97% (当前正在还原由 "System Writer" 报告的文件)
总体进度 - 97% (当前正在还原由 "System Writer" 报告的文件)
总体进度 - 98% (当前正在还原由 "System Writer" 报告的文件)
还原由 "System Writer" 报告的文件已完成
还原由 "NTDS" 报告的文件已完成
总体进度 - 99% (当前正在还原由 "WMI Writer" 报告的文件)

恢复摘要:
---------------------

还原系统状态成功完成[2008/6/1 18:07]

成功还原文件日志
"C:\Windows\Logs\WindowsServerBackup\SystemStateRestore 01-06-2008 17-42-15.log
"

请重新启动计算机以完成该操作。
注意: 当您重新启动服务器时, 系统状态恢复将尝试恢复
很多系统文件, 这需要几分钟时间才能完成, 具体取决于
被替换的文件数量。计算机可能会在此过程中重新启动多次。
请耐心等待, 并且请勿打断重新启动过程。

C:\Users\Administrator.LXH>_
```

图 4.44　提示需要重新启动系统

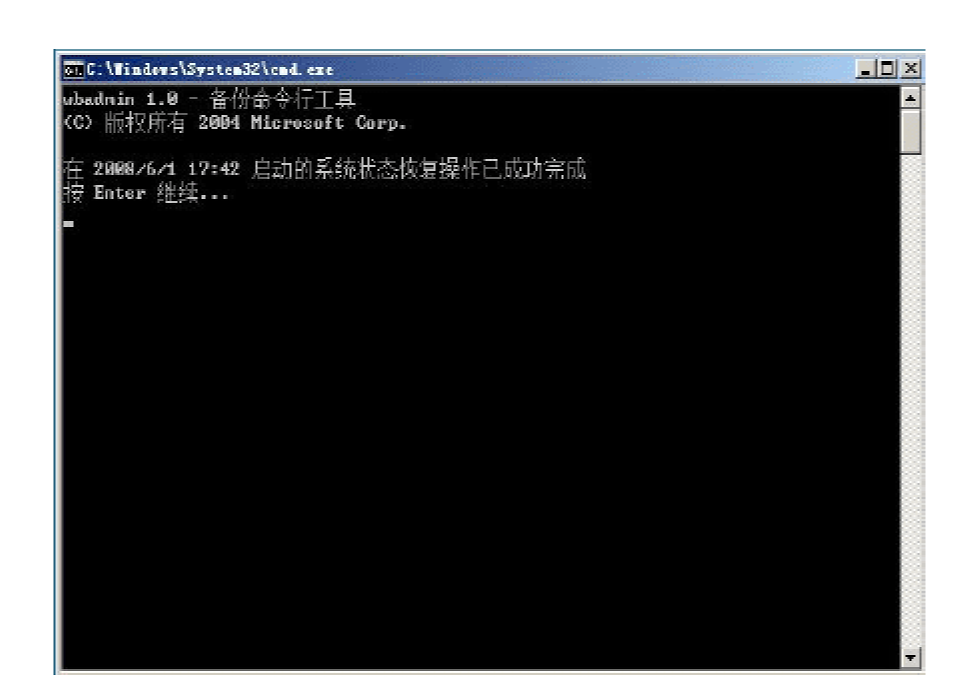


图 4.45　恢复操作已完成

小　　结

活动目录（Active Directory）是指存储网络资源信息的目录，AD DS 域服务是 Windows Server 2008 的核心服务。本章主要介绍了 AD DS 域服务的安全功能及应用，包括 RODC 的应用、权限委派、用户帐户权限审核等。用户帐户是常用的目录对象之一，合理分配每个用户帐户的访问控制权限是网络安全的主要任务。权限继承是活动目录管理中不可或缺的部分，它可帮助管理员快速部署用户权限，但多重继承也可能导致权限混乱，从而引发安全漏洞。权限委派功能可避免权利过分集中，提高网络安全性，减轻了管理员的工作负担。

默认情况下，域与域之间是无法正常访问的，域中的用户要想自由访问网络中不同域的服务器，需要在不同域间创立信任关系。通过委派，让信任用户可以在一个特定容器内改变属性、创建或删除某种类型的对象以及更改某种类型对象的某些属性等。

习　　题

1. 如何为对象设置和取消权限继承？
2. 如何对 AD DS 进行域服务配置？
3. 按照组作用域的不同，可以将组分为哪几类，功能有何区别？
4. 简要介绍什么是权限委派，可以委派的权限包括哪些？

实验：应用 RODC 缓存用户信息

实验目的

掌握 RODC 在网络安全管理中的应用。

实验内容

为现有可读写域控制器 coolpen.net，部署一台 RODC 域控制器，并将指定的用户帐户密码缓存到 RODC 数据库中。

实验步骤

1. 打造安全的 Windows Server 2008 服务器操作系统。
2. 将 coolpen.net 的林功能级别提升为 Windows Server 2008 或 Windows Server 2003。
3. 部署 RODC 域控制器。
4. 添加缓存帐户信息。

第 5 章

用户帐户安全

用户帐户是通知 Windows 用户可以访问哪些文件和文件夹，可以对计算机和个人首选项进行哪些更改的信息集合。使用用户帐户，可以多人共用同一台计算机，但仍然保留自己的文件和环境设置。每个人都可以使用用户名和密码访问其用户帐户。在 Windows Server 2008 系统中，管理员可以创建多个用户帐户，通过设置不同的系统访问权限和操作权限从而保证计算机系统和网络的安全。

本章导读

- 系统管理员帐户管理
- 用户帐户管理
- 用户帐户安全
- 用户帐户控制

5.1 系统管理员帐户管理

系统管理员帐户（默认名称为 Administrator）是 Windows 系统中的特殊帐户，它拥有对系统的绝对访问权限，可以直接删除、修改或添加普通用户帐户。拥有管理员权限，也就拥有了整个网络和系统的生杀大权，这也使得管理员帐户成为黑客的主要攻击目标。而对于猜测管理员帐户名和密码的攻击方式，普通的防火墙软件和策略是无法预防的，最好的方法就是加强对系统帐户的安全管理。

5.1.1 系统管理员密码设置

在早期的 Windows 2000 Server 网络中，对系统管理员帐户密码是没有强制要求的，用户可以根据习惯选择是否使用密码，也可以根据习惯使用哪种密码。在 Windows Server 2003 系统中允许管理员帐户不设置密码，不同的是管理员可以通过配置帐户安全策略，提高用户帐户密码的安全性。在 Windows Service 2008 系统中，默认已经启用了密码的复杂性要求，并且要求安装过程中设置强密码。同时，为了确保管理员帐户安全，建议管理员定期更换帐户密码。

1. 注意事项

在设置管理员帐户密码时，应注意以下问题：

- 切不可让账号与密码相同。如果将用户账号与密码设置为相同，许多系统扫描工具默认将帐户和密码作为相同的设置扫描系统，无疑会省去攻击者的很多力气；
- 切不可使用自己的姓名。对于本单位和熟悉本单位的人而言，姓名无疑是攻击的首选，因为这几乎谁都能猜得到。另外，在许多黑客编写的字典中，往往将百家姓一一列出，并放在字典的前列；
- 切不可使用英文词组。一些常用或别致的英文单词往往是用户设置密码时的最爱，这类密码既便于记忆，又凸显自己的个性。但事实上，黑客也早已猜到并详细地将其编入字典，因此，建议不要使用英文词组；
- 切不可使用特定意义的日期。以具有特定意义的日期作为密码是任何人都十分喜爱的，这一类日期通常是自己生日、父母生日、儿女生日、朋友生日、重大节日、个人纪念日等。不用说熟悉的人可以猜得到，即使是陌生人也可以通过穷举的方式而得手。在黑客字典中，几乎全部罗列以上所有的几个组合，实在令人惊骇不已；
- 切不可使用简单的密码。字符数越少、密码越简单，在破解时所用的时间就越短。一个以穷举软件每秒钟可以重试 10 万次之多，字数越少，字符越简单化，排列组合的结果也就越少，也就越容易被攻破。

2. 安全密码原则

欲保证帐户密码的安全，应当遵循以下原则：

- 用户密码应包含英文字母的大小写、数字、可打印字符，甚至是非打印字符，将这些符号排列组合使用，以期望达到最好的保密效果；
- 用户密码不要太规则，不要将用户姓名、生日和电话号码作为密码。不要用常用单词作为密码；
- 根据黑客软件的工作原理，参照密码破译的难易程度，以破解需要的时间为排序指标，密码长度设置时应遵循 7 位或 14 位的整数倍原则；
- 在通过网络验证密码过程中，不得以明文方式传输，以免被监听截取；
- 密码不得以明文方式存放在系统中，确保密码以加密的形式写在硬盘上，且包含密码的文件是只读的。加密的方法很多，如基于单向函数的密码加密，基于测试模式的密码加密，基于公钥加密方案的密码加密，基于平方剩余的密码加密，基于多项式共享的密码加密，基于数字签名方案的密码加密等。经过上述方法加密的密码，即使是系统管理员也难以获得；
- 密码应定期修改，避免重复使用旧密码，并采用多套密码的命名规则；
- 建立账号锁定机制。一旦同一账号密码校验错误若干次即断开连接并锁定该账号，经过一段时间才解锁；
- 由网络管理员设置一次性密码机制，用户在下次登录时必须更换新的密码。

3. 系统帐户密码要求

通常情况下，Windows Server 2008 系统对用户帐户密码要求如下：

- 不包含全部或部分的用户帐户名；
- 长度至少为 6 个字符；
- 包含来自以下 4 个类别中的 3 个字符：
  - 大写英文字母（从 A 到 Z）；
  - 小写英文字母（从 a 到 z）；
  - 10 个基本数字（从 0 到 9）；
  - 非字母字符（例如，!、$、#、%）。

对于未安装 Active Directory 服务 Windows Server 2003 计算机或修改了 Windows Server 2003/2008 默认组策略的计算机，其用户帐户密码可以随意设置。

强密码具有以下特征：

- 长度至少有 7 个字符；
- 不包含用户的生日、电话、用户名、真实姓名或公司名等；
- 不包含完整的字典词汇；
- 包含全部下列 4 组字符类型：大写字母（A,B,C…）、小写字母（a,b,c…）、数字（从 0~9）、非字母字符（键盘上所有未定义为字母和数字的字符，如` ~ ! @ # $ % ^ & * ( ) _ +

-={}|[]\:";'<>?,./)。

除此之外，管理员帐户的密码应当定期修改，尤其是当发现有不良攻击时，更应及时修改复杂密码，以避免被破解。为避免密码因过于复杂而忘记，可用笔记录下来，并保存在安全的地方，或随身携带避免丢失。其实，最安全的方法就是不使用常规密码，而采用电子密钥等一些几乎无法破解的登录方式，确保系统安全性。

5.1.2 系统管理员帐户管理

除了设置管理员帐户复杂密码外，用户还可以通过更改默认帐户名称、设置陷阱等方法来保证用户帐户的安全。

1. 更改 Administrator 帐户名

由于 Administrator 是系统默认的，所以黑客攻击服务器时总是试图获取 Administrator 帐户和密码来获取最高权限，其后果可想而知。通常情况下，可以通过更改管理员帐户名称来降低被破解的概率，从而提高系统的安全性。

方法一：在组策略中更改

01 以 Administrator 帐户登录本地计算机，依次选择“开始”→“运行”命令，在“运行”对话框中输入“gpedit.msc”命令，单击“确定”按钮，显示如图 5.1 所示“本地组策略编辑器”对话框。

02 单击“计算机配置”，依次展开“Windows 设置”→“安全设置”→“本地策略”→“安全选项”选项。在“安全选项”右侧双击“重命名系统管理员账号”选项，显示如图 5.2 所示“帐户：重命名系统管理员帐户 属性”对话框，更改系统管理员账号后点击“确定”按钮，最后重启系统生效。



图 5.1 “本地组策略编辑器”对话框

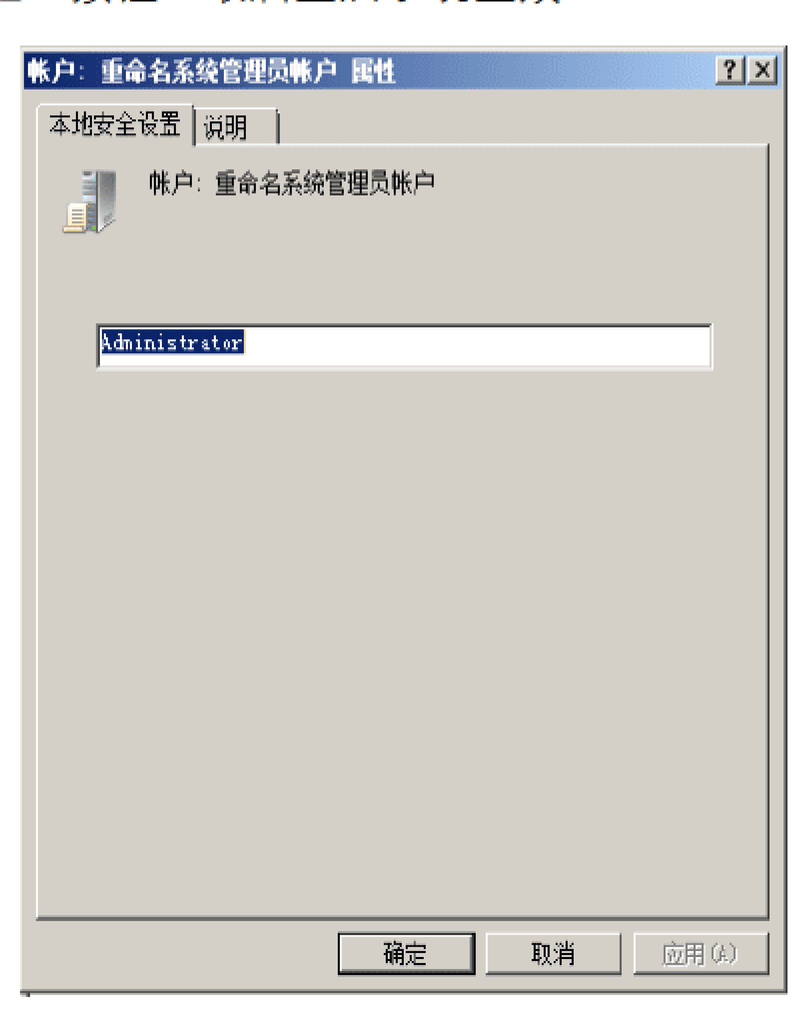


图 5.2 “帐户：重命名系统管理员帐户 属性”对话框

方法二：在“计算机管理”控制台中更改

以 Administrator 帐户登录本地计算机，依次单击“开始”→“管理工具”→“计算机管

理”选项，打开“计算机管理”窗口，依次展开“本地用户和组”→“用户”选项，右击 Administrator 帐户并选择“重命名”选项，输入新的帐户名即可，如图 5.3 所示。

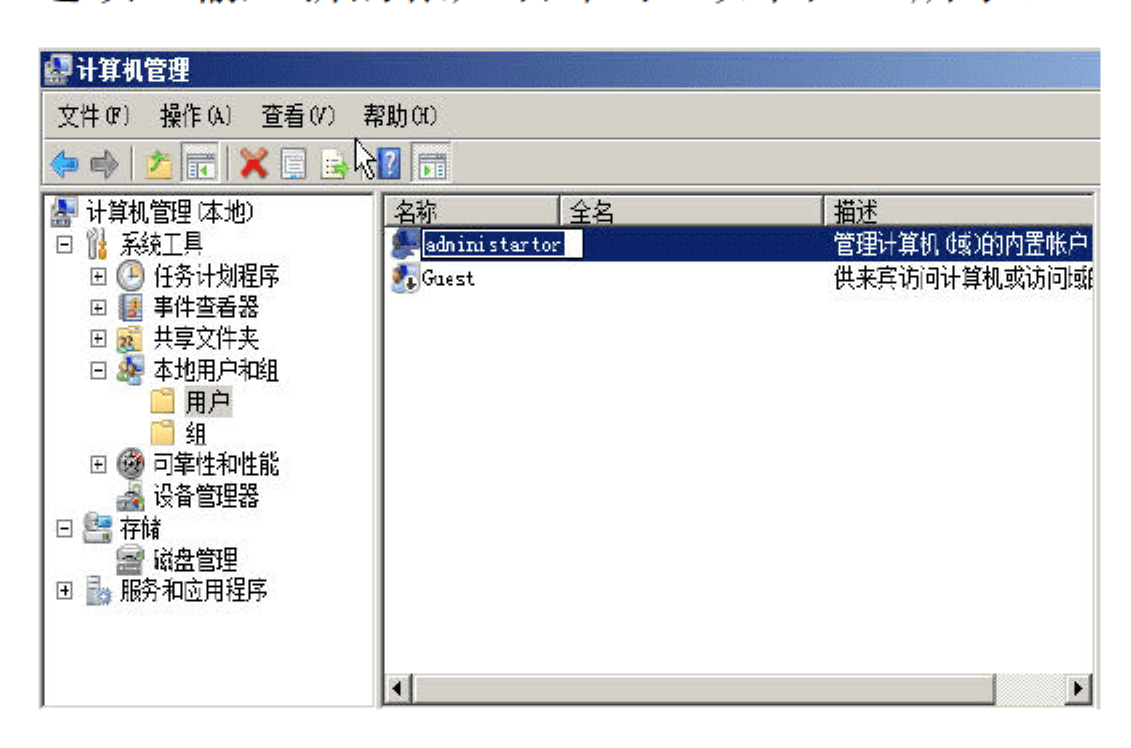


图 5.3 “计算机管理”对话框

提示 在更改新的帐户名称时，应避免使用 admin、user、master 之类作为管理员的帐户名，否则帐户的安全性同样无法得到有效的保障。

如果是域控制器，则可以依次选择“开始”→“管理工具”→“组策略管理”命令，找到作用于根域的默认策略“Default Domain Policy”，右击并选择快捷菜单中的“编辑”命令，打开“组策略管理编辑器”窗口。依次展开“计算机配置”→“策略”→“安全设置”→“本地策略”→“安全选项”选项，双击右侧主窗口中最下面的“帐户：重命名系统管理员帐户”策略，打开如图 5.4 所示“帐户：重命名系统管理员帐户 属性”对话框，系统默认是没有定义该策略的，选中“定义这个策略设置”复选框，并在文本框中输入新的名称即可。

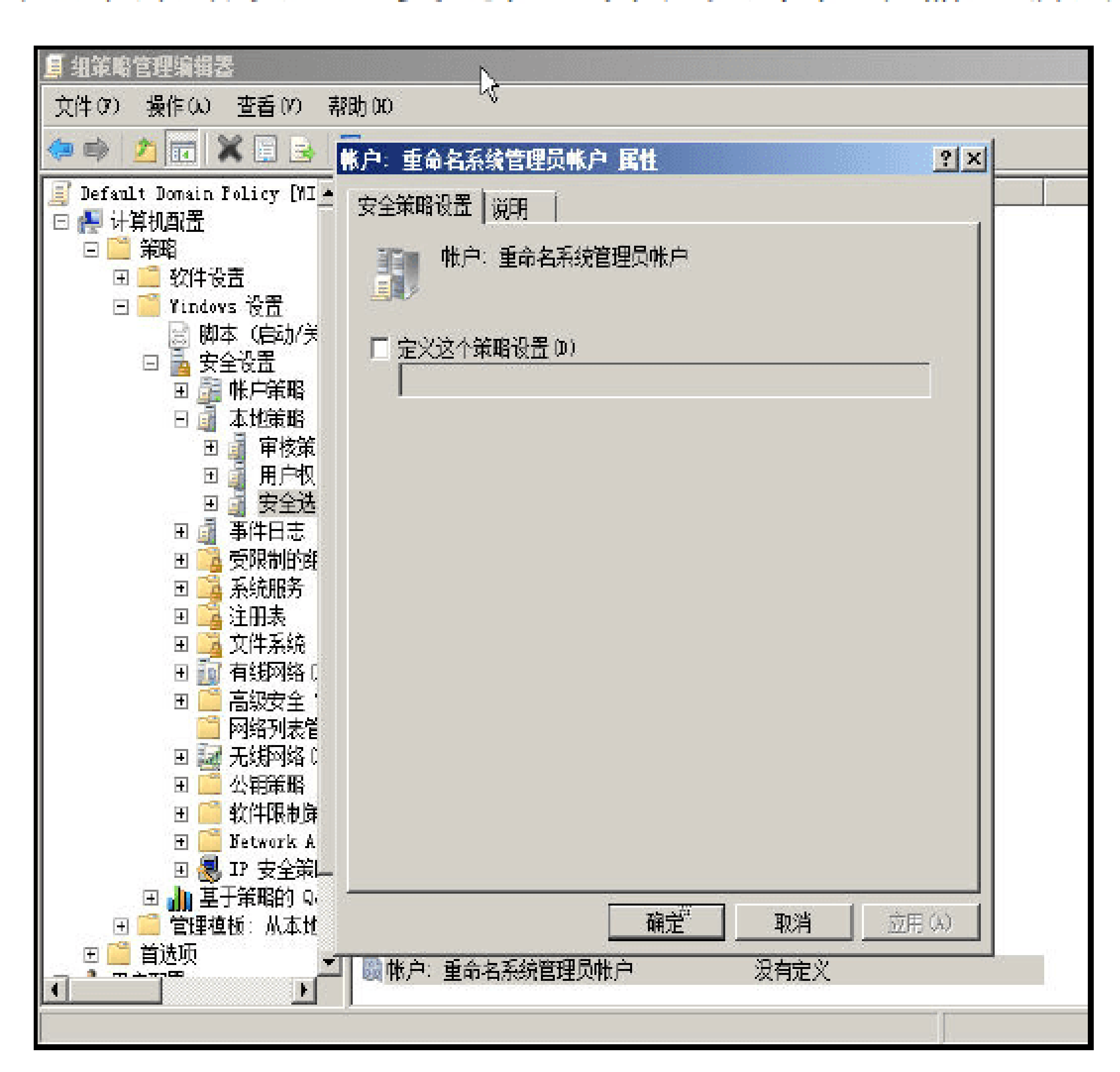


图 5.4 “帐户：重命名系统管理员帐户 属性”对话框

2. 设置“陷阱”账号

所谓“陷阱”账号主要是针对最易遭受攻击的 Administrator 帐户而言的。管理员可以先指定一个系统管理员帐户（区别于 Administrator 帐户），然后创建一个名称为 Administrator 的普通帐户，赋予其极低的访问和操作权限，同时设置超强的帐户密码，从而避免入侵者对真正

管理员帐户的攻击。

01 选择“开始”→“管理工具”→“计算机管理”命令，在“计算机管理”窗口中依次展开“本地用户和组”→“用户”选项。右击“用户”创建一个以 Administrator 为用户名的用户，其密码设置为超过 16 位的复杂密码，显示如图 5.5 所示“新用户”对话框，此用户名不会和原来的 Administrator 帐户重复，因为 SID 是不同的。

02 把刚创建的 Administrator 这个用户加入 Guests 组，即赋予陷阱帐户最低的权限，如图 5.6 所示。当黑客试图获取 Administrator 账号时，不仅可以延长入侵时间，给管理员预留充足的响应时间，而且就算他拿到了陷阱帐户的账号密码后，也不能进行其他更改操作。

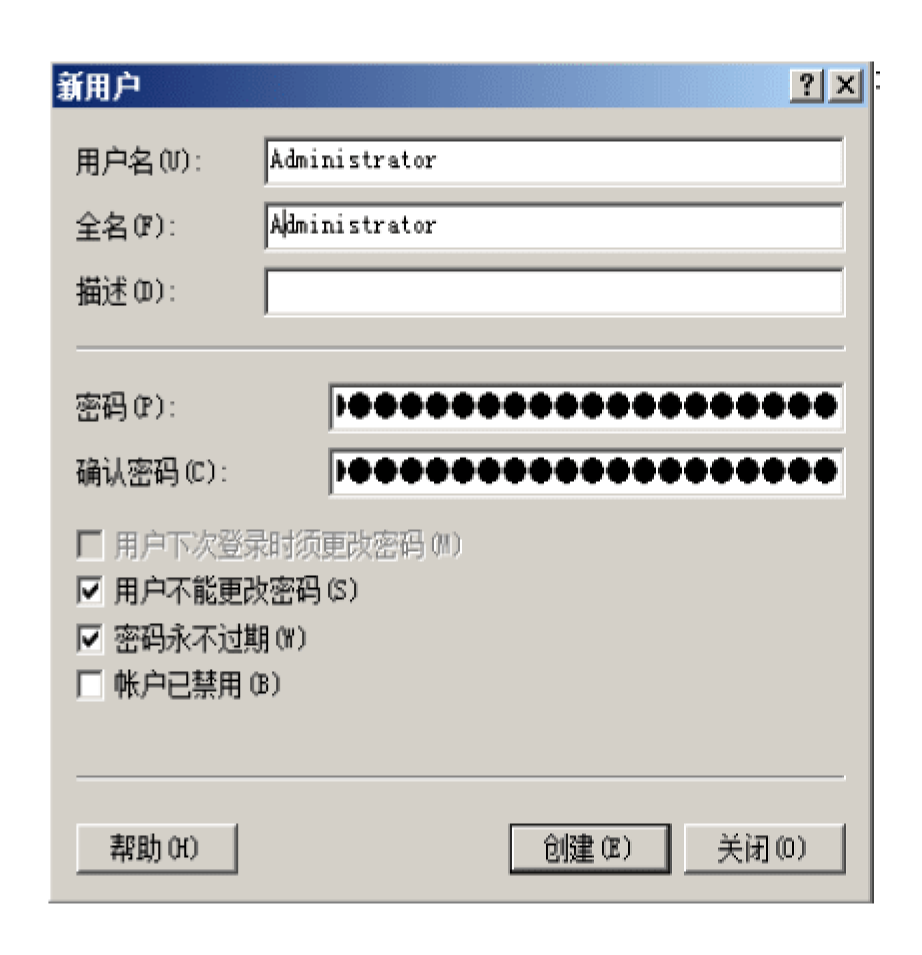


图 5.5 “新用户”对话框

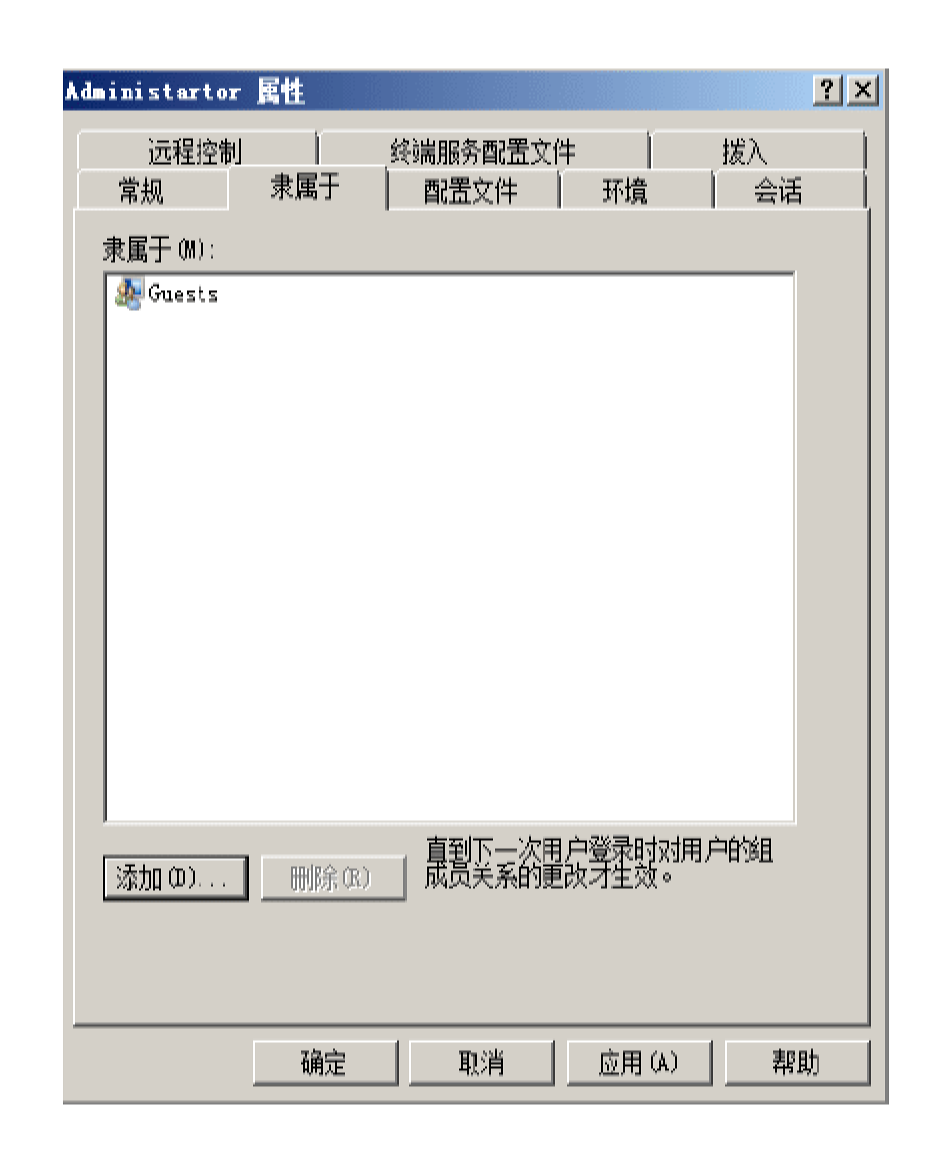


图 5.6 “Administrator 属性”对话框

03 单击“确定”按钮，保存设置即可。

5.1.3 备份和还原系统帐户

如果 Windows Server 2008 系统瘫痪，则所有账号信息都会自动丢失，而解决的办法是重新安装 Windows Server 2008 系统，通过手工方法将原有用户账号信息恢复成功并非一件容易的事，因此，保护用户账号信息就成为网络管理员必须认真面对的“课题”。Windows Server 2008 提供的系统账号备份和恢复工具，可以帮助管理员轻松解决问题。

1. 对系统账户进行备份

01 单击“开始”按钮，在“开始搜索”文本框中，输入“credwiz”命令并回车，启动“存储的用户名和密码”向导，依次单击“下一步”按钮，选择操作类型和保存路径，如图 5.7 所示。在“存储的用户名和密码”对话框中，选择“备份存储的用户名和密码”单选按钮。

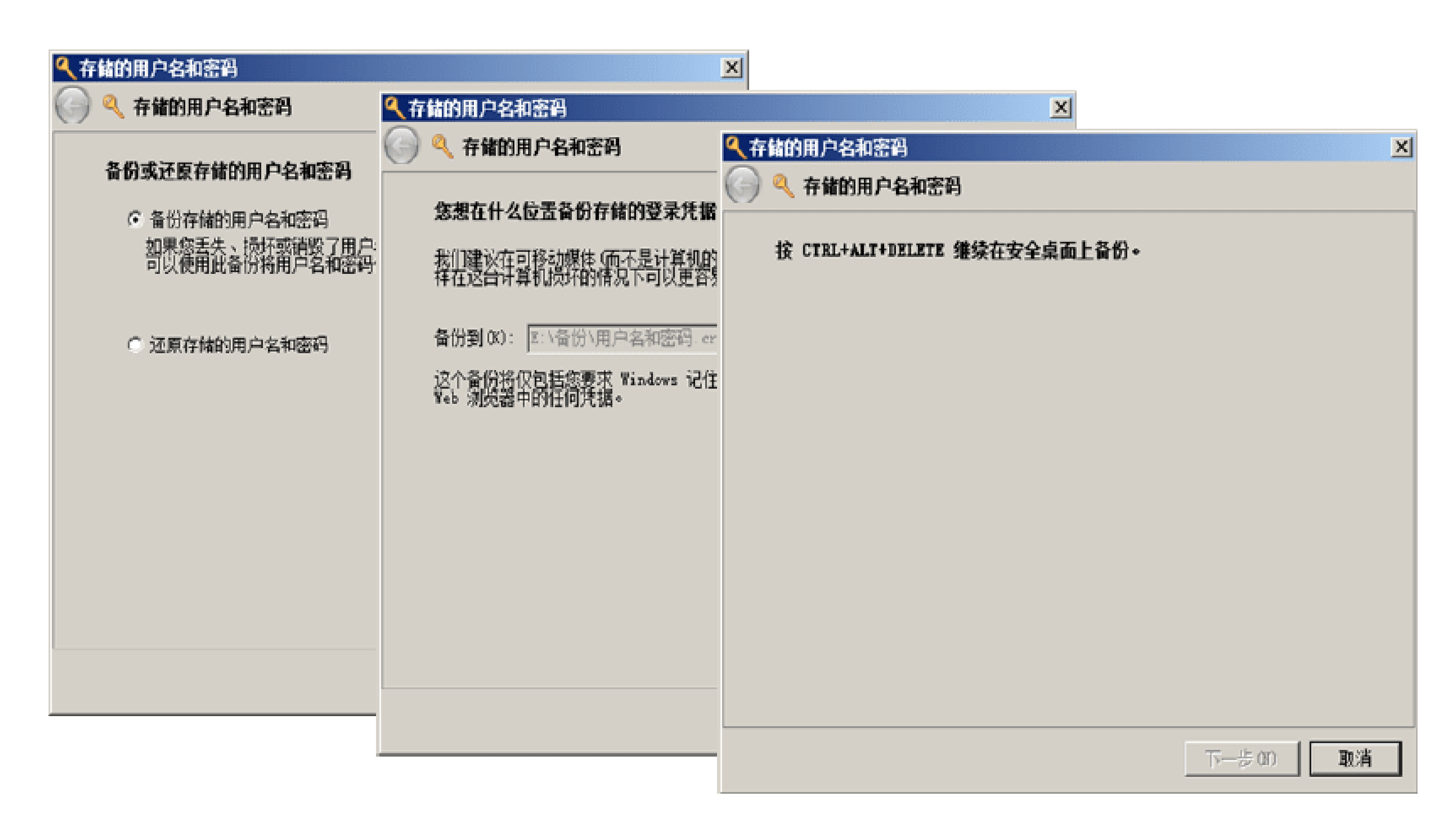


图 5.7　选择操作类型和存储备份的路径

02 根据提示信息按下“CTRL＋ALT＋DELETE”组合键，在“使用密码保护备份文件”对话框中，输入希望设置的密码。单击“下一步”按钮，即可完成系统用户帐户信息的备份，如图 5.8 所示。

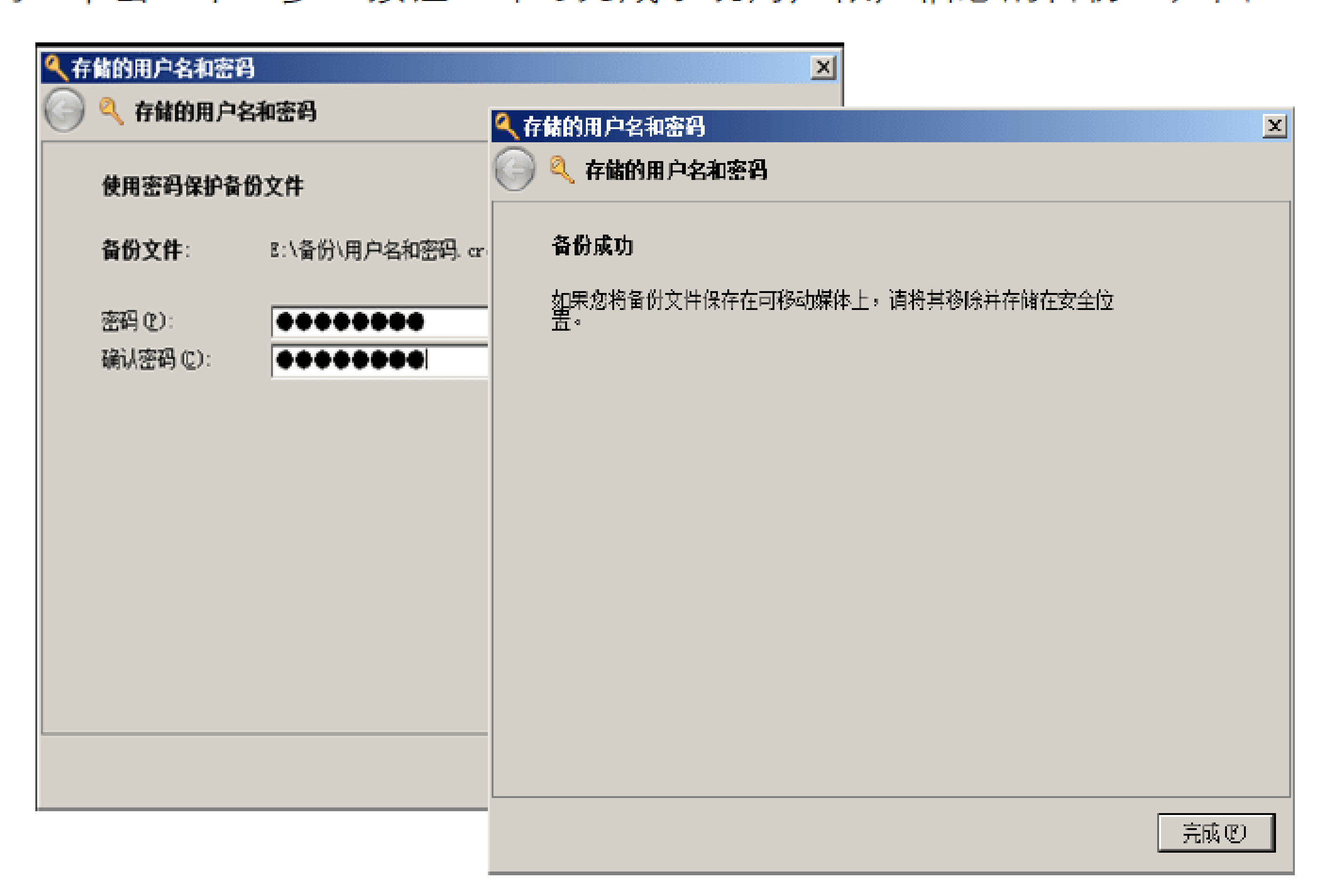


图 5.8　备份用户名和密码向导

03 系统自动生成一个名为“用户名和密码”的备份文件。妥善保管此文件即可。

2. 对系统账户进行还原

如果 Windows Server 2008 系统中的用户账号信息丢失、损坏甚至销毁时，管理员可以通过还原将受损的系统账号恢复到原先的正常状态。

01 单击“开始”按钮，在“开始搜索”文本框中，输入“credwiz”命令并回车，启动“存储的用户名和密码”向导，选中“还原存储的用户名和密码”单选按钮，单击“下一步”按钮，选择保存备份文件的路径，如图 5.9 所示。

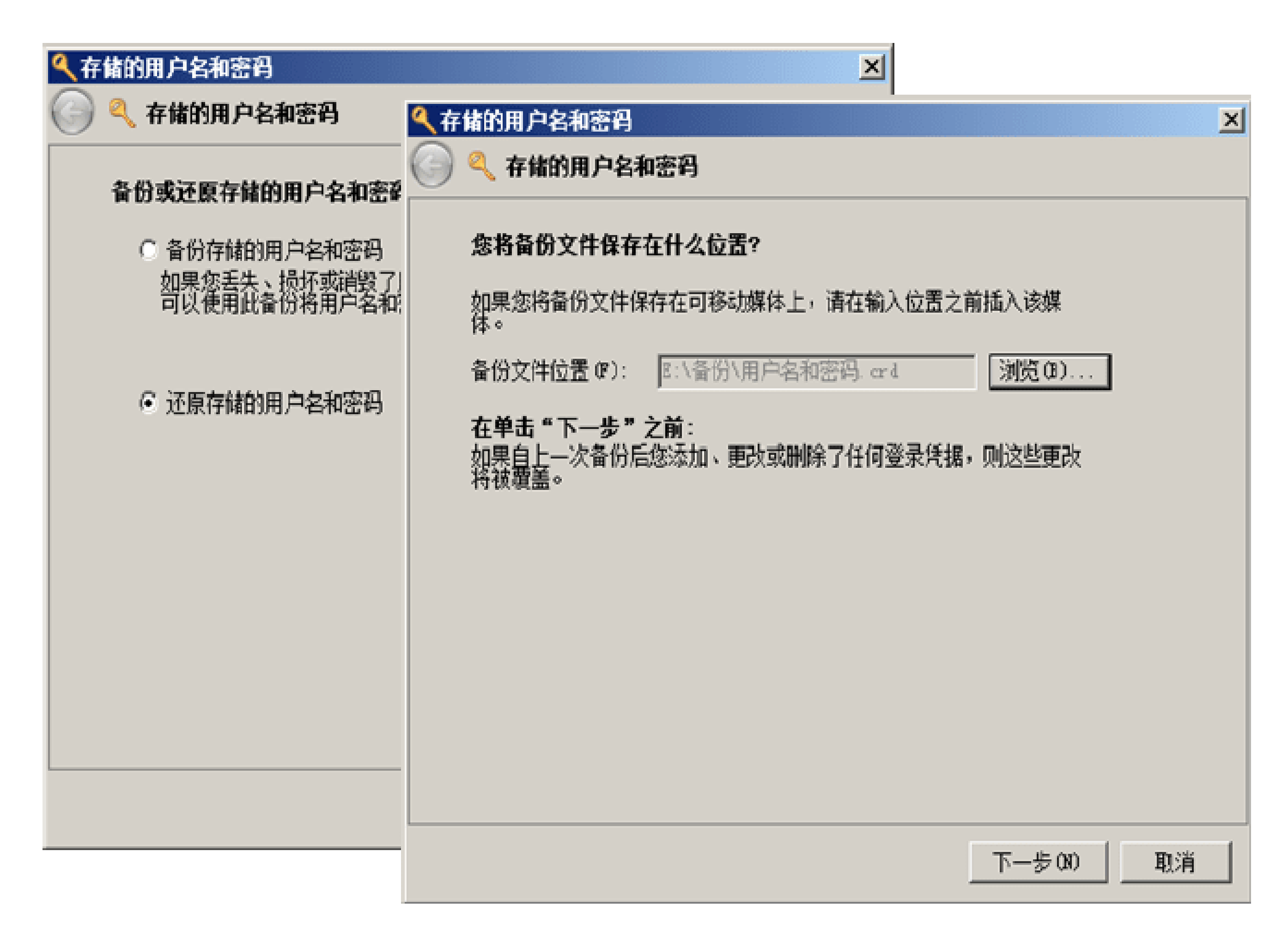


图 5.9　还原用户名和密码

02 根据提示信息，按下“CTRL＋ALT＋DELETE”组合键，输入创建备份文件时设置的密码即可，如图 5.10 所示。

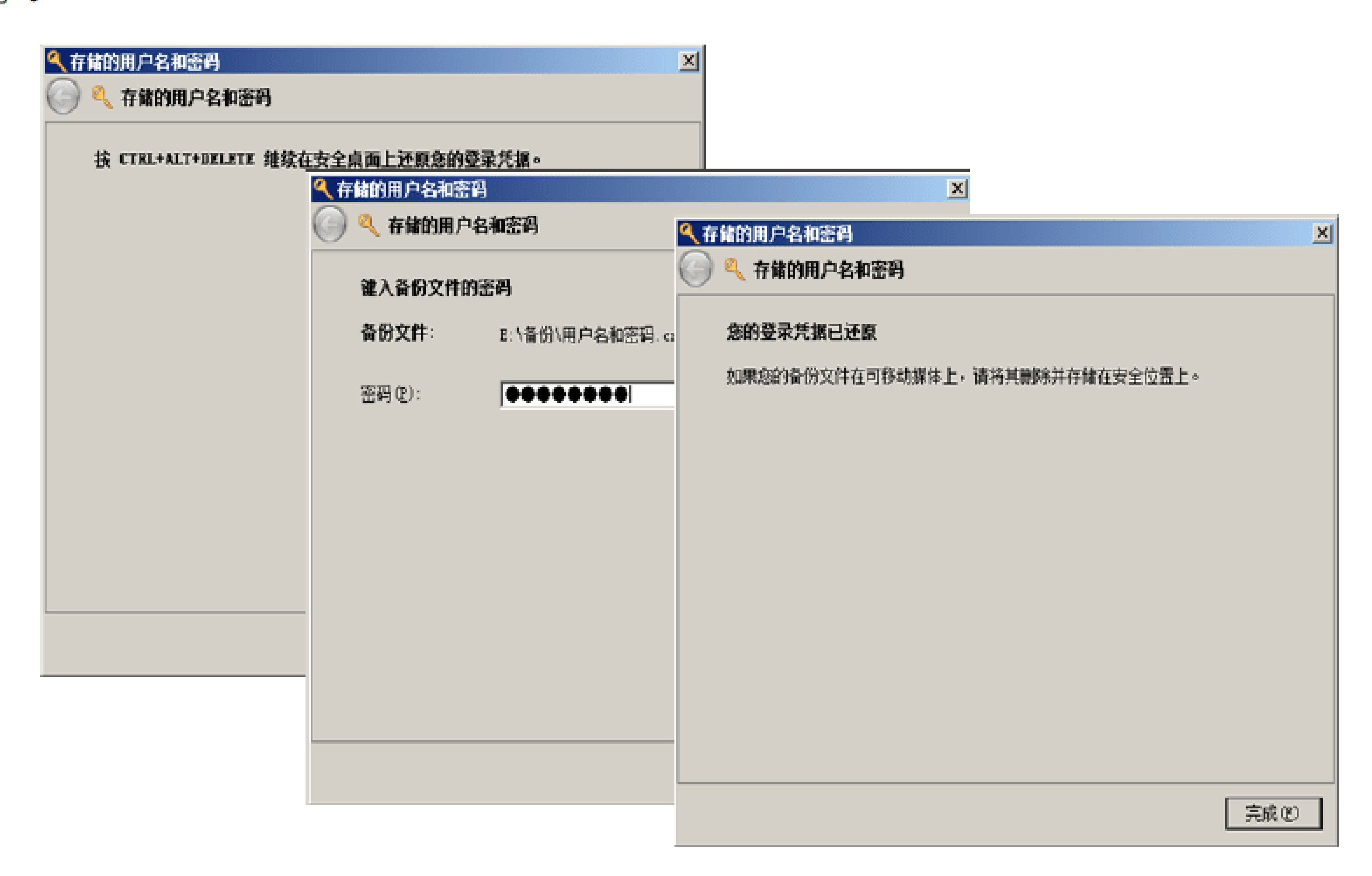


图 5.10　成功还原用户名和密码

5.2　用户帐户管理

除管理员帐户之外，还应为其他用户创建一些普通帐户，如来宾帐户、个人用户帐户等。为了确保系统或网络的安全，普通用户帐户的安全设置也是不可小视的，如果操作不当很容易导致安全漏洞。例如，管理员必须根据用户的实际身份和管理职能，及时调整其对应帐户身份。如果用户暂时离开网络，则可以先停用其帐户，以免被滥用。

5.2.1　启用、禁用、删除用户帐户

帐户和用户是相互对应的。如果新用户加入，需要创建新的帐户；如果有些帐户临时不用，则可以暂时将其禁用，以免被其他用户滥用；如果用户完全脱离者计算机或域，则可以删除对应帐户。每个用户帐户都可能对系统安全造成威胁，通常情况下只保留够用的帐户即可。

1. 禁用、启用和删除本地用户帐户

以具有管理员权限的帐户登录系统，打开“计算机管理”的“用户”窗口，双击需要禁用的用户帐户，打开用户帐户的属性对话框，在“常规”选项卡中，选中“帐户已禁用”复选框，如图 5.11 所示。单击“确定”按钮即可禁用该帐户。取消勾选“帐户已禁用”复选框，即可重新启用已禁用的帐户。

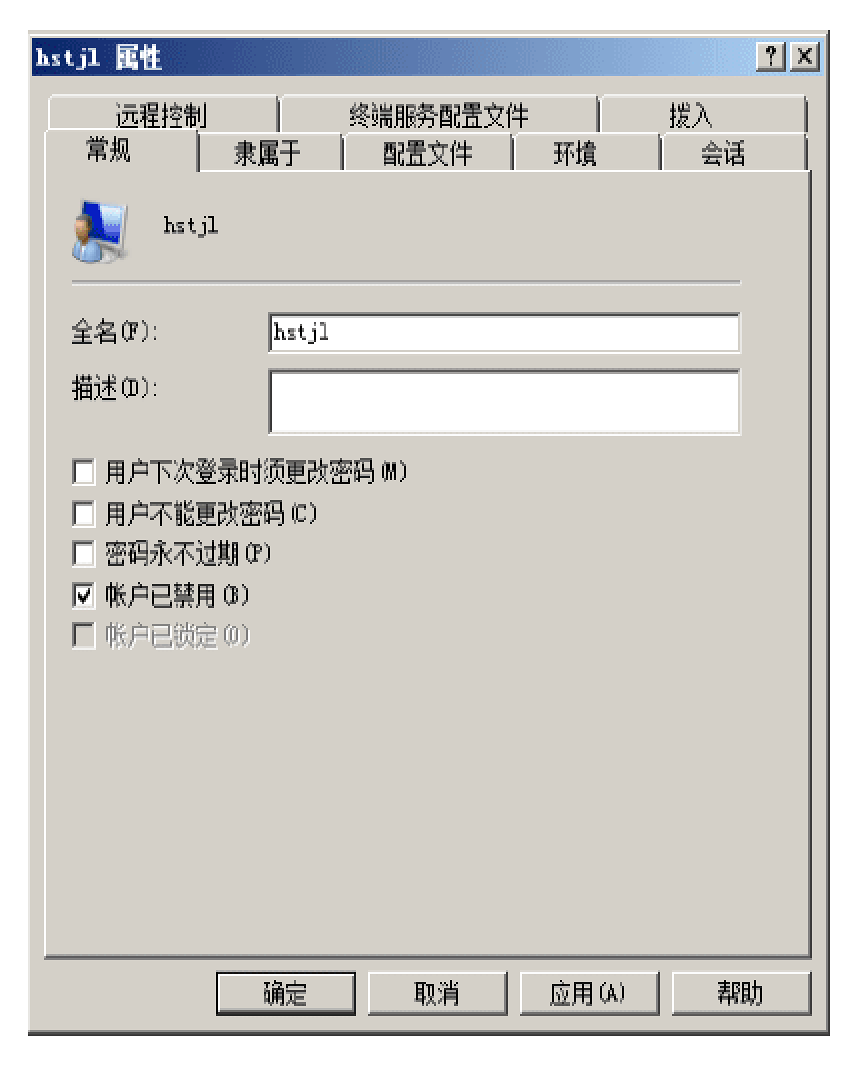


图 5.11　禁用本地用户帐户

提示　除非有特殊应用，Guest 帐户应当被禁用。事实上，许多网络攻击就是借助 Guest 用户来实现。即使启用 Guest 帐户，也应当为其指定最低的访问权限。

在“计算机管理”窗口中，右击需要删除的帐户，选择“删除”选项，显示如图 5.12 所示“本地用户和组”对话框，单击“是”按钮，即可删除所选帐户。

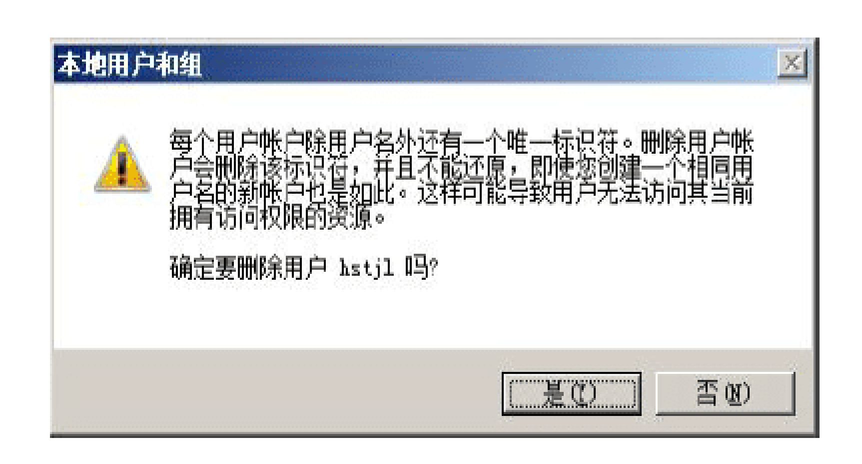


图 5.12　“本地用户和组”对话框

2. 禁用、启用和删除域用户帐户

以具有管理员权限的帐户登录控制器，打开“Active Directory 用户和计算机”窗口，右击

想要禁用的用户帐户，选择快捷菜单中的“禁用帐户”选项即可将其禁用，如图 5.13 所示。

用户帐户被禁用以后，便不能再登录。如果想启用用户帐户，则可以按照相同的方法，选择快捷菜单中的“启用帐户”选项即可。如果帐户不再使用，或需要重设所有权限，可将其删除，右击用户帐户名，并选择快捷菜单中的“删除”选项即可删除该帐户。

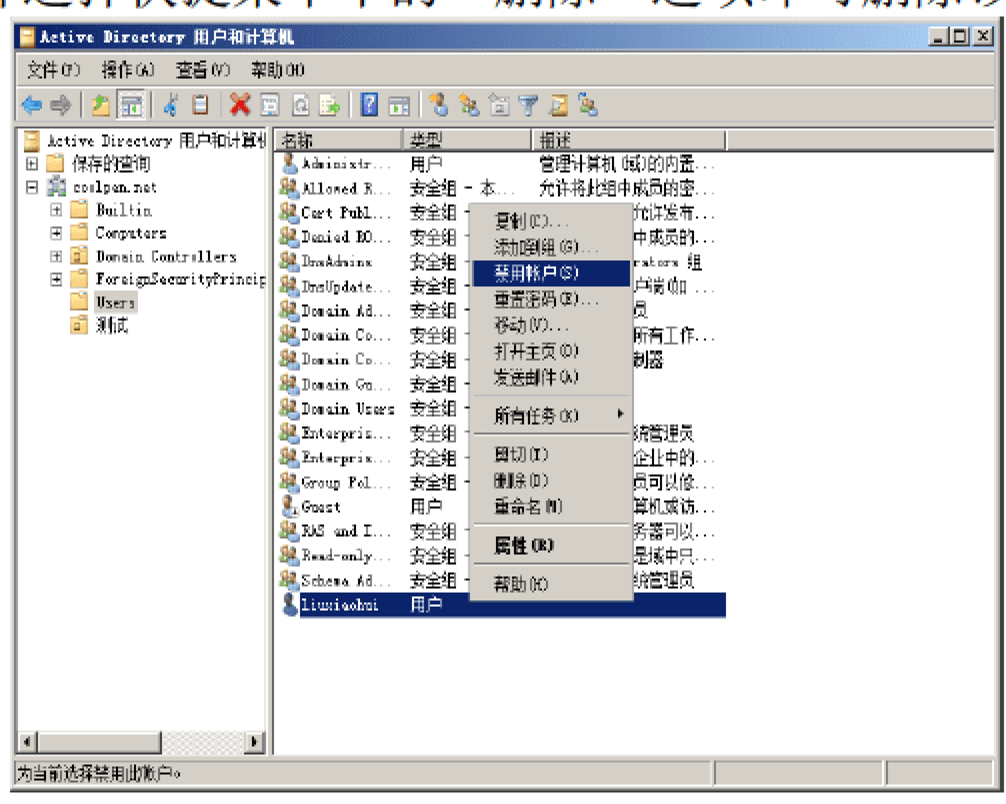


图 5.13　禁用域用户帐户

5.2.2　限制用户可以登录的时间

默认情况下，域用户帐户可以随时登录到域控制器，但是为了确保服务器系统以及网络的安全，应对用户帐户的登录时间进行限制。该限制仅适用于域用户帐户，本地用户帐户登录系统时间无法限制。

01 在“Active Directory 用户和计算机”窗口中，双击要设置的用户，打开用户属性对话框。单击“登录时间”按钮，显示如图 5.14 所示“liuxiaohui 的登录时间”对话框，默认允许在任何时间登录。

02 在登录时间分布表中，框选拒绝登录的时间范围，选择“拒绝登录”单选按钮，如图 5.15 所示。例如，本例中设置的是 liuxiaohui 帐户，在每周星期一到星期五的 9 点至 17 点范围内登录域控制器。

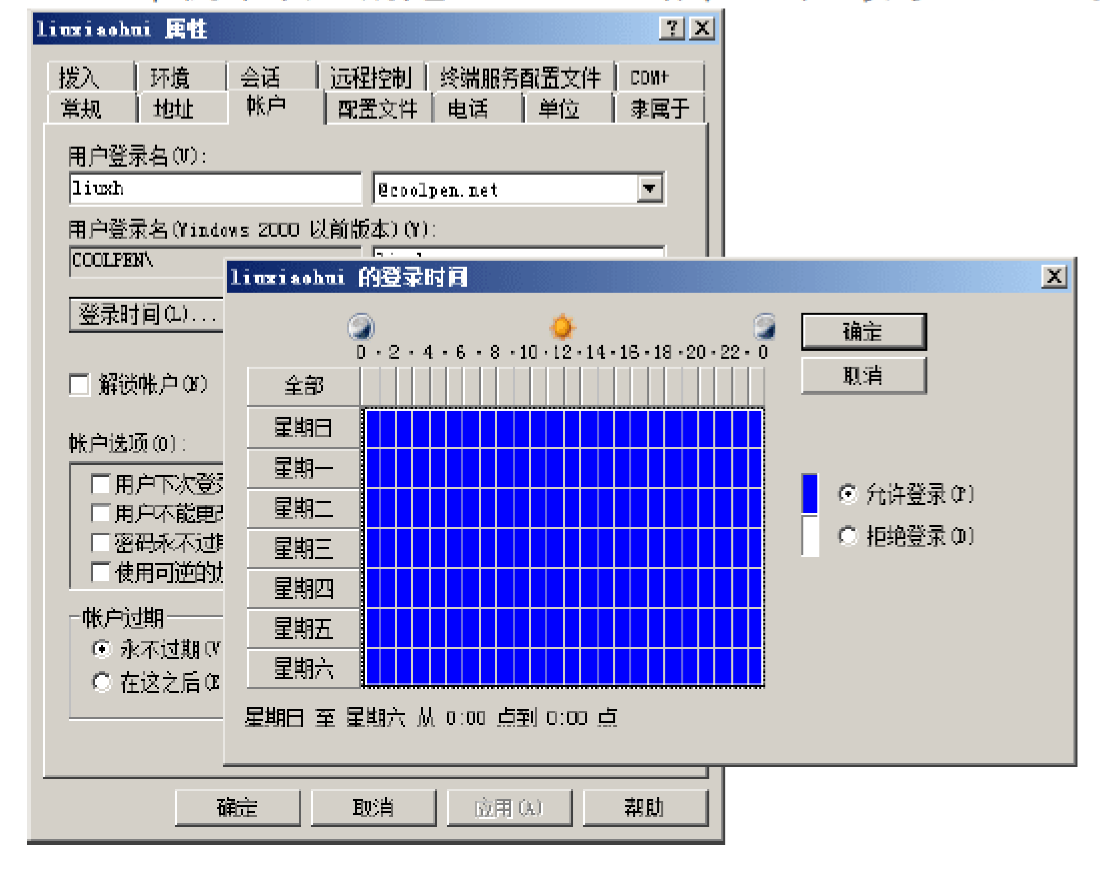


图 5.14　设置 liuxiaohui 的登录时间

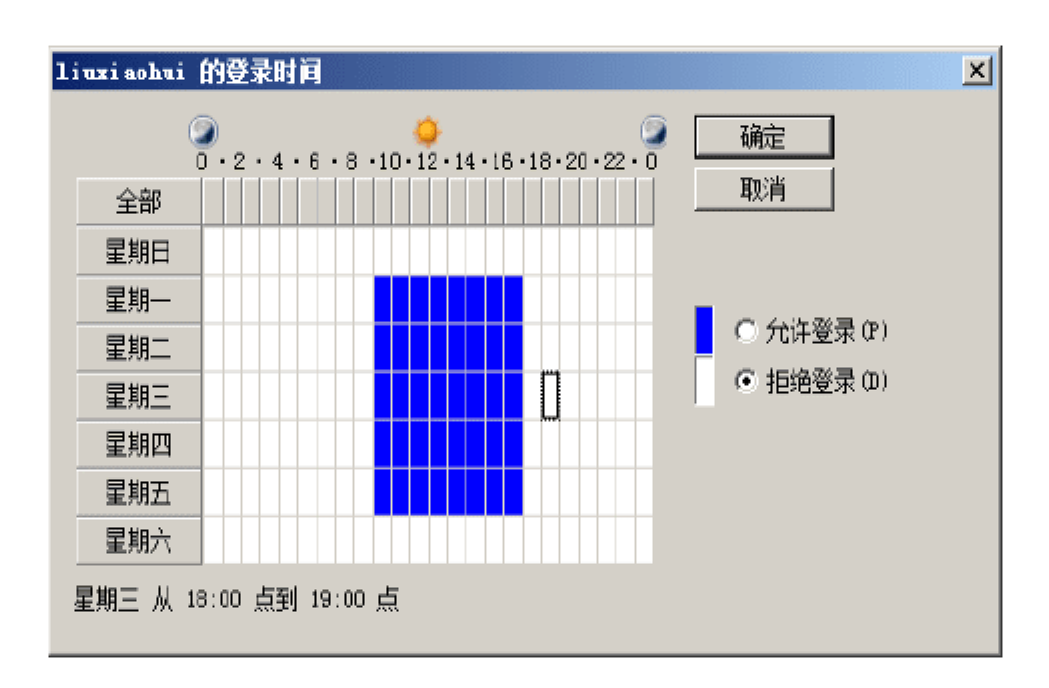


图 5.15　设置登录时间

03 单击“确定”按钮保存设置。

5.2.3 限制用户可以登录的工作站

限制用户登录到的工作站，是指限制用户帐户只能从网络中指定的计算机上登录，访问 Active Directory 中的资源。默认情况下，域用户帐户可以从网络中任意计算机上登录，通过将用户帐户和登录计算机捆绑在一起，可以实施更加有效的安全管理措施。

01 仍然以 liuxiaohui 帐户为例，在“liuxiaohui 属性”对话框的“帐户”选项卡中，单击“登录到”按钮，显示如图 5.16 所示“登录工作站”对话框。默认选中“所有计算机”单选按钮，即允许用户登录网络中的所有计算机。

02 选择“下列计算机”单选按钮，在“计算机名”文本框中输入允许登录的工作站的 NetBIOS 名称，单击“添加”按钮添加到列表中，可以添加多个允许登录的工作站名称。

03 单击“确定”按钮保存设置。

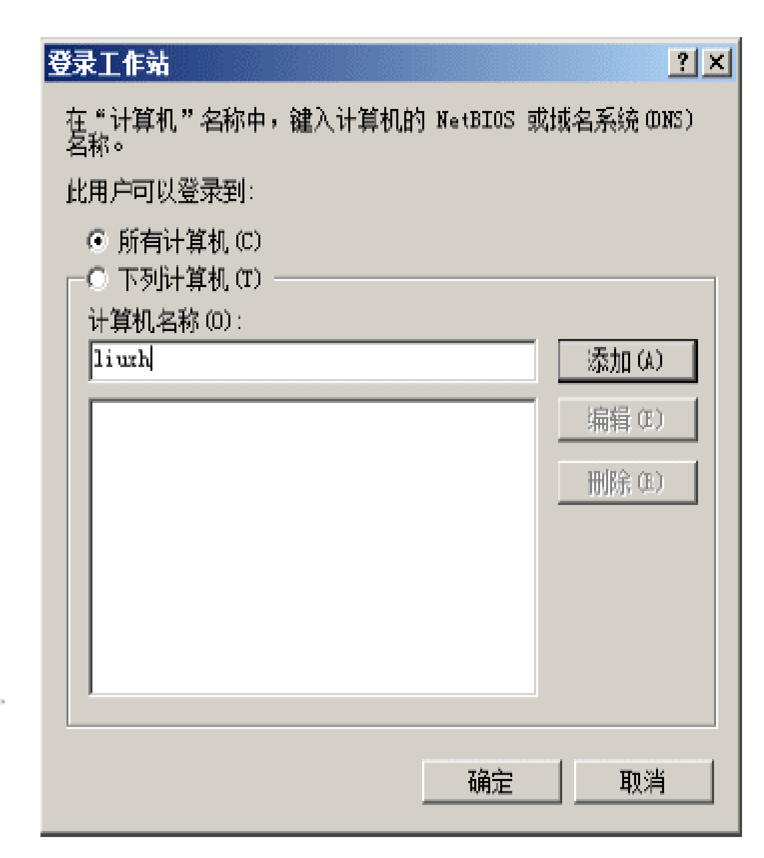


图 5.16 “登录工作站”对话框

5.2.4 恢复误删除的域用户

在 Windows Server 2008 的“Active Directory 用户和计算机”管理控制台中，没有提供对误删除的用户恢复功能。管理员可以借助“Adrestore.exe”工具，在命令行模式下恢复删除的用户，该工具支持 Windows Server 2000/2003/2008 系统中的活动目录。本例以恢复被删除的“Testuser”用户为例，介绍“Adrestore.exe”工具恢复用户的方法。

01 将该工具复制到运行 AD DS 域服务的计算机中，选择“开始”→“所有程序”→“附件”→“命令提示符”选项，显示如图所示的“命令提示符”窗口，并切换到存储“Adrestore.exe”工具的目录下，输入如下命令：

Adrestore /r

回车，命令成功执行，显示如图 5.17 所示窗口，该命令枚举活动目录中删除的对象，并显示用户完整的 FQDN 信息。

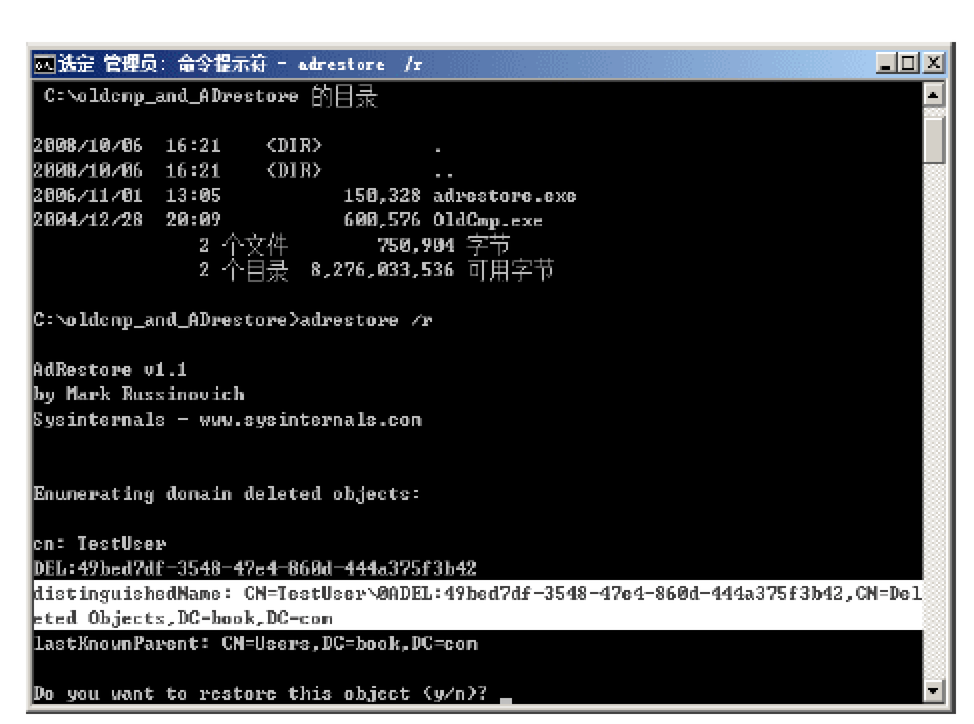


图 5.17 枚举活动目录中被删除的对象

02 输入“Y”，恢复删除的用户信息，提示用户被成功恢复，如图 5.18 所示。同样的方法可以恢复其他被删除的 Active Directory 对象。

03 打开“Active Directory 用户和计算机”窗口，选择“Active Directory 用户和计算机”→“book.com”→“Users”选项，显示 “Active Directory 用户和计算机”窗口，“TestUser”被成功恢复，恢复的用户状态为“禁用”，如图 5.19 所示。

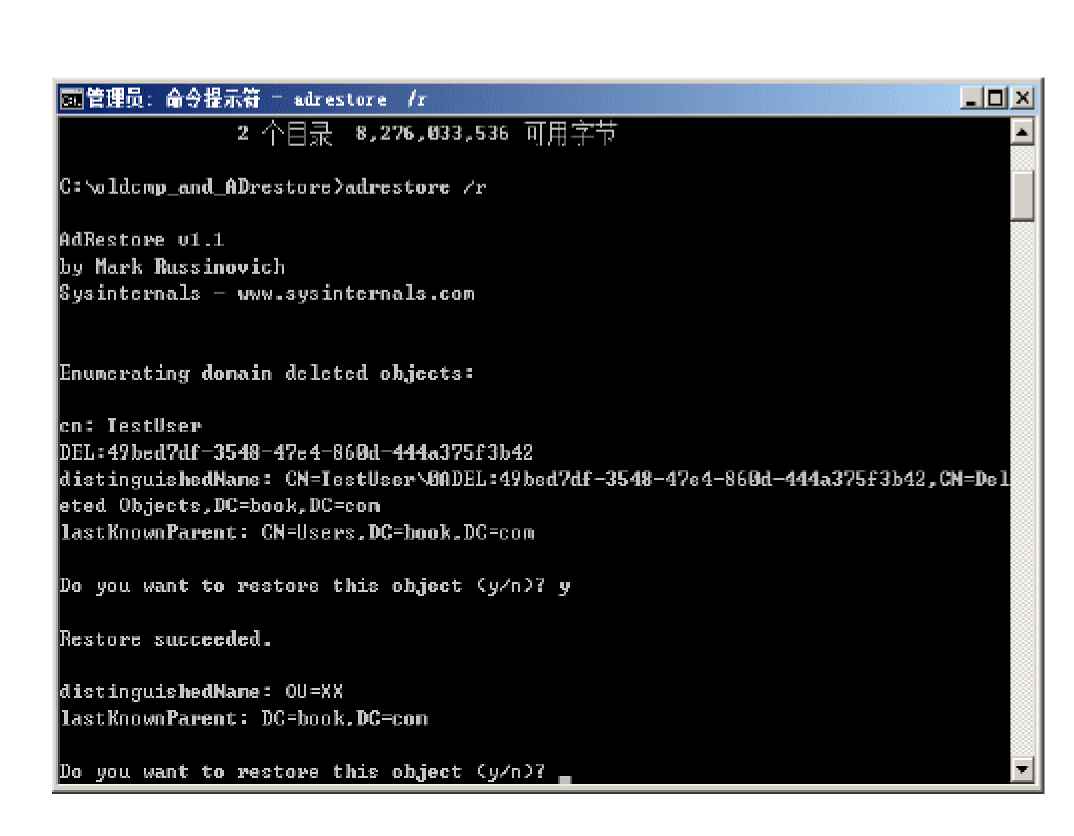


图 5.18　恢复误删除的用户

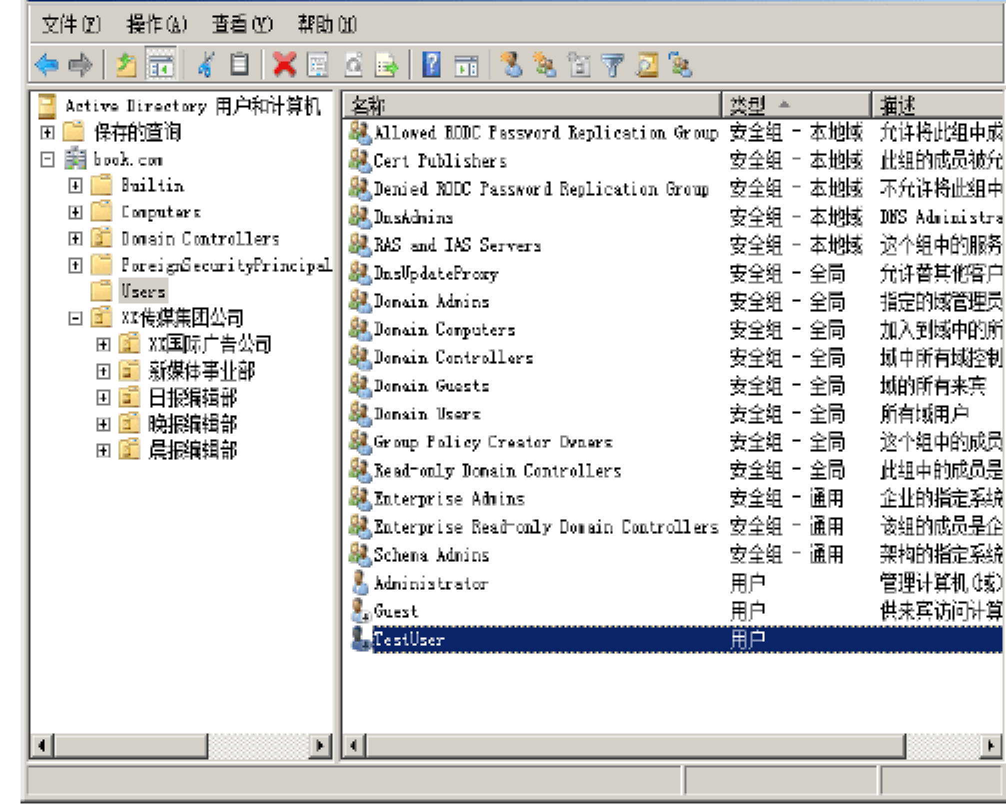


图 5.19　被删除用户已被恢复

04 恢复的帐户需要重新设置密码，启用该帐户即可完整恢复被删除的用户帐户。

5.3　管理密码

设置一个高强度的安全密码固然重要，但是密码的管理也是非常重要的。在 Windows Server 2008 系统中，管理员可以通过设置密码策略，强制网络用户帐户的密码符合某些条件，或者强制定期更改其密码。另外，无论是独立工作站、域控制器还是客户端，都应注意定期更改登录密码，并妥善保存用户帐户密码。

5.3.1　设置密码策略

默认情况下，Windows Server 2008 系统已经启用了用户帐户密码策略，如图 5.20 所示。这些策略的主要作用就是指导用户设置符合要求的强安全密码，管理员可以根据需要调整密码策略的值，例如系统默认策略要求密码最常使用期限为 42 天，而为了确保帐户密码安全，可以设置为 30 天。

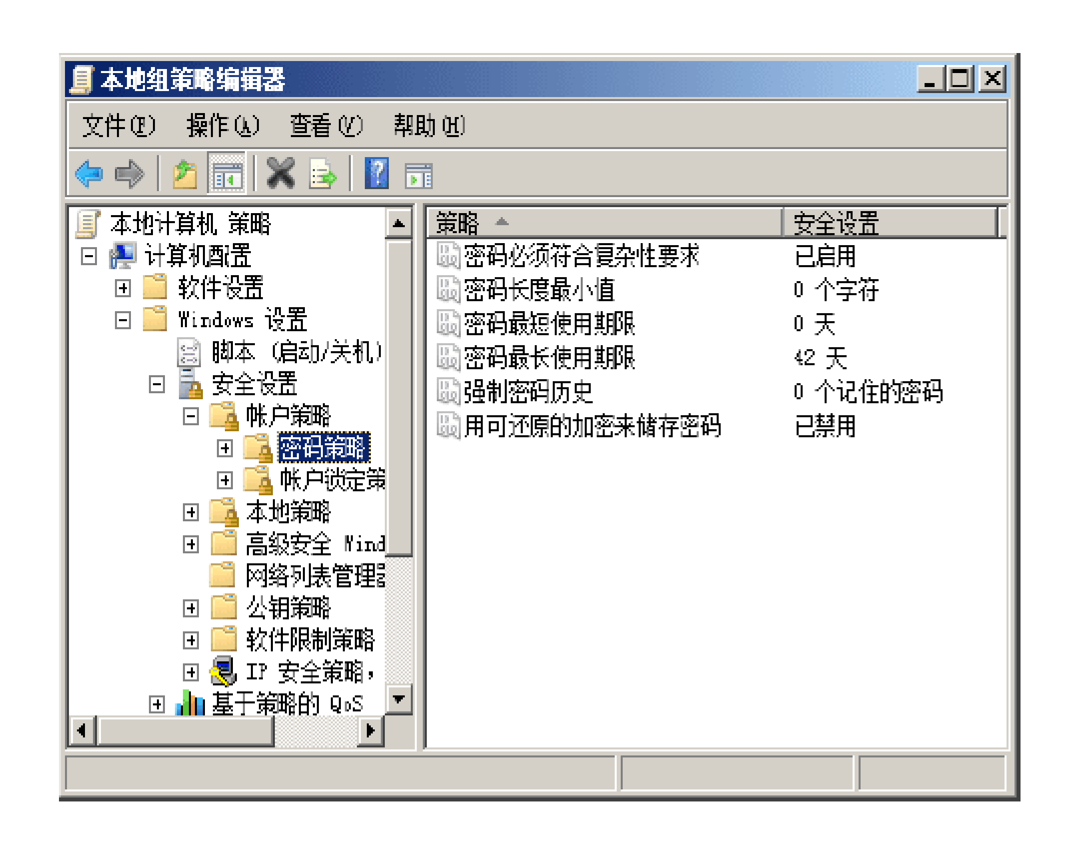


图 5.20　密码策略



提示　有关帐户密码策略的详细设置，请参考本书“第 6 章　组策略安全”中的介绍。

5.3.2　重设用户密码

密码是用户登录系统和网络的唯一凭证，如果丢失密码也就无法登录。为了确保用户可以继续使用原帐户，管理员必须为其重新设置密码。另外，即使没有丢失密码，也应定期更换不同的密码，以免因密码使用时间过长而被别人窃取。

1. 设置本地用户密码

默认情况下，本地计算机的系统管理员帐户，可以随时通过“计算机管理”工具更改所有用户帐户的登录密码，而其他用户则无此权限，只能通过更改密码向导实现。

（1）管理员帐户重设普通帐户密码

01 打开“计算机管理”窗口，展开“本地用户和组”→“用户”，右击需要更改密码的用户帐户，选择快捷菜单中的“设置密码”选项，显示“为 hstjl 设置密码”对话框。单击“继续”按钮，显示如图 5.21 所示对话框，在“新密码”和“确认密码”编辑框中输入新密码。

02 单击“确定”按钮，显示如图 5.22 所示“本地用户和组”提示框。



图 5.21　为 hstjl 设置密码

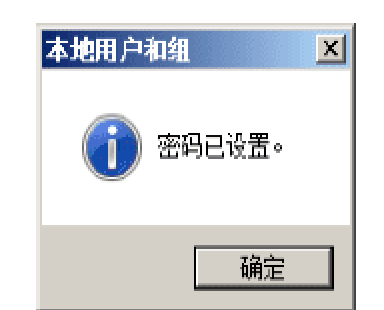


图 5.22　“本地用户和组”提示框



提示　由于用户加密文件和个人安全证书中都包含了原来的密码信息，更改后将无法访问这些加密文件，失去个人安全证书的访问权。除非用户帐户密码丢失，建议管理员慎重使用该方式为成员用户重设密码。

（2）普通帐户重设自己密码

01 登录想要更改密码的用户帐户，按下“Ctrl+Alt+Del”组合键打开如图 5.23 所示窗口，类似于 Windows Server 2003 系统的“Windows 安全”窗口。

02 单击“更改密码”按钮，打开如图 5.24 所示对话框，只有正确输入旧密码后，新密码才可以生效。在“旧密码”文本框中输入用户帐户的当前密码，在“新密码”和“确认密码”文本框中输入新的密码即可。

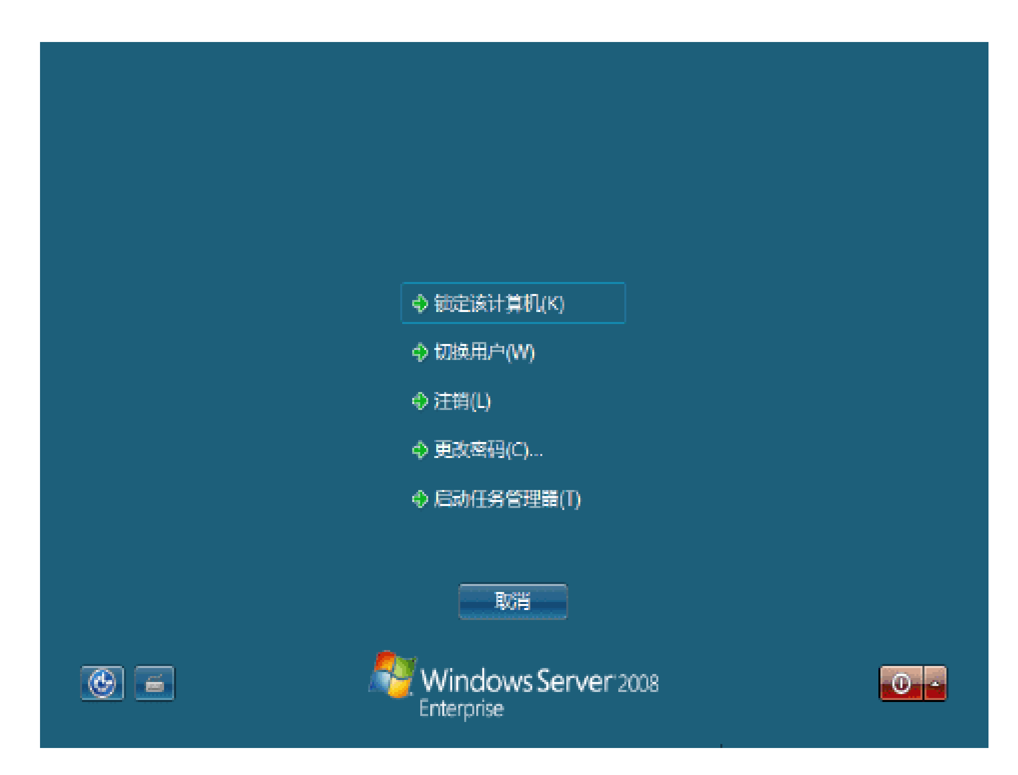


图 5.23　Windows 安全

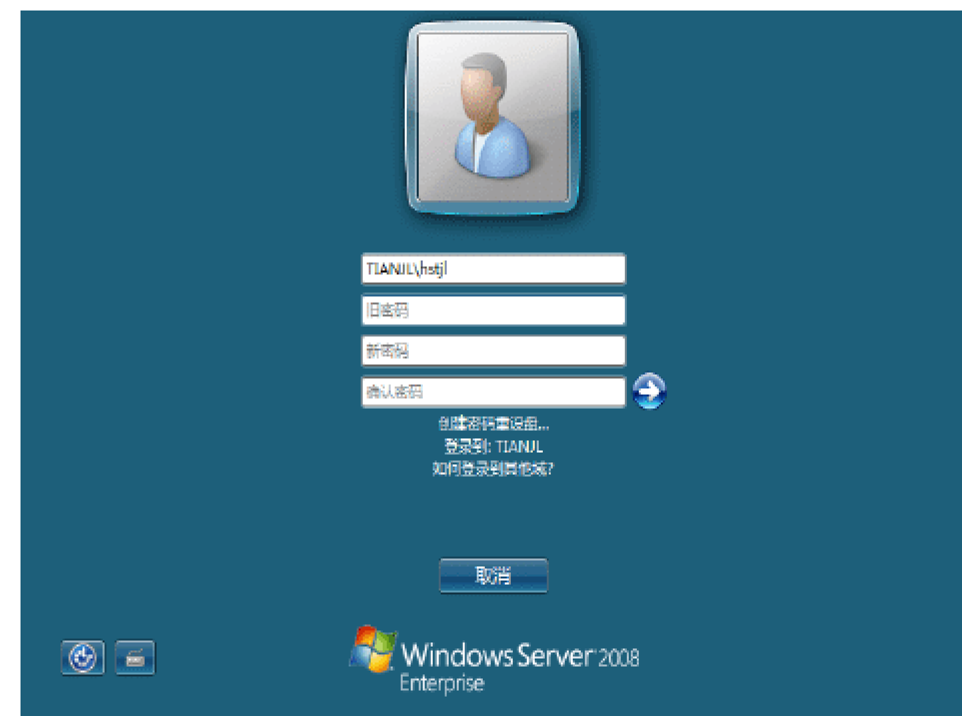


图 5.24　更改密码

03 单击“确定”按钮，修改成功，显示如图 5.25 所示对话框。

04 单击“确定”按钮，返回 Windows 资源管理器。



图 5.25　更改密码

（3）创建密码重置盘

“创建密码重置盘”是确保帐户密码安全的重要手段，创建过程中会将用户帐户和密码信息，以加密的方式存储到指定的软盘或 U 盘上。忘记登录密码时，使用这些信息可以重新创建一个新的安全密码，实现登录系统的目的。

01 在“更改密码”窗口中，单击“创建密码重置盘”链接，启动“忘记密码向导”。依次单击“下一步”按钮，选择用于保存密码的软盘、可移动硬盘并输入当前使用的用户帐户密码，如图 5.26 所示。

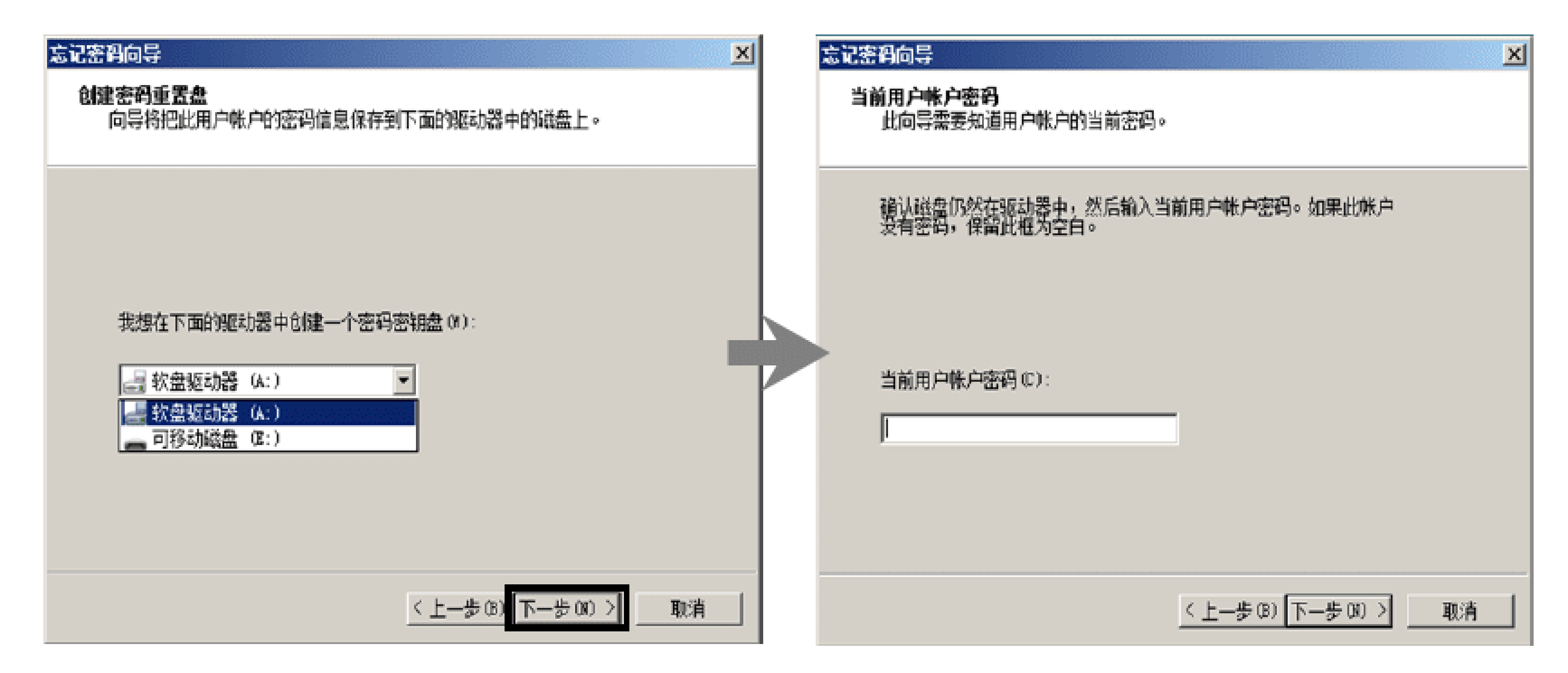


图 5.26　创建密码重置盘

02 单击“下一步”按钮，开始创建，稍等即可完成。需要注意的是，任何人都可以通过密码重置盘，重新设置当前用户帐户的密码，因此应做好标记，并妥善保管。

如果忘记此用户帐户的密码，可以在登录界面中选择用户帐户后，单击“重设密码”链接启动“重置密码向导”，根据提示信息插入密码重置盘，当运行至如图 5.27 所示“重置用户帐

户密码”步骤时，重新设置新的密码即可，此时还可以设置一个密码提示信息。

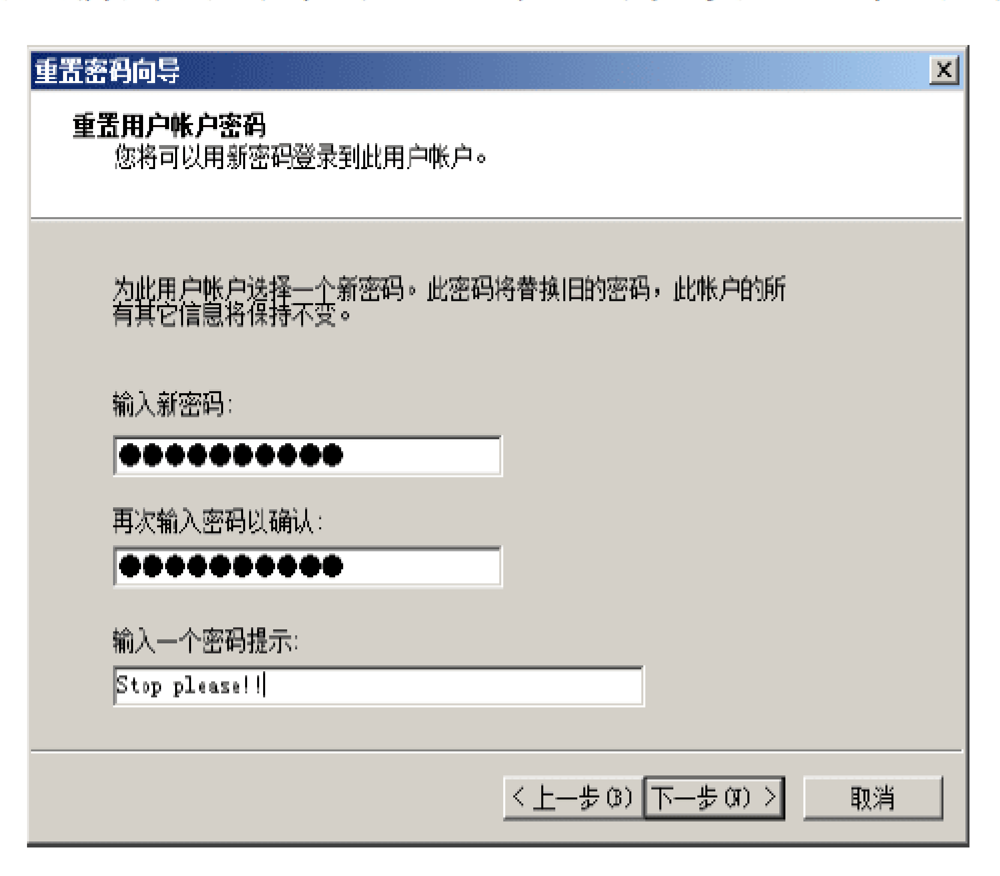


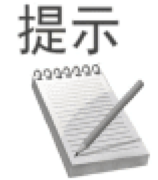
图 5.27　“重置用户帐户密码”对话框

2. 设置域用户帐户密码

在域环境中重设帐户密码比较简单。使用具有相关权限的管理员帐户登录到域控制器，打开“Active Directory 用户和计算机”窗口。在“Users”容器中，右击想要重置密码的用户帐户，选择快捷菜单中的“重置密码”选项，显示如图 5.28 所示“重置密码”对话框，在“新密码”和“确认密码”文本框中输入新密码，单击“确定”按钮即可。使用这种方法，也可以重设管理员帐户的密码。



图 5.28　“重置密码”对话框

提示 

如果当前帐户已被锁定，则可以选中“解锁用户的帐户”复选框，使密码更改立即生效。系统默认配置的安全策略，可能会限制用户更改密码的次数或登录次数限制，如果超出策略限制，立即锁定帐户，并等待一定时间后自动解锁。此时，对应用户可以告知管理员，由管理员登录到域控制器，使用该方式为其重设密码并解锁帐户。

5.4　用户权限安全

使用用户帐户可以登录到域或其他计算机中，从而获得对计算机资源的网络资源的访问权。经常访问网络的用户都应拥有网络唯一的用户帐户，并且根据用户的职责不同，分配不同的用户权限，同时，设置严格的用户策略，保护用户帐户的安全。

5.4.1 用户特权

用户执行特定任务的权利，通常会影响整个计算机系统，而不只是某个目录对象。特权作为计算机安全设置的一部分，由管理员指派给单个用户或用户组。要减轻用户帐户的管理任务，应该对组帐户指定特权，而不是对单个用户帐户。

1. 可授予用户的特权

对组帐户指定特权时，当用户成为该组成员时将自动指派那些特权。这种管理特权的方法比为每个用户帐户指定单独的权限要容易得多。如表 5.1 所示是可以授予用户的特权以及相关说明。

表 5.1 可授予用户的特权

特权	说明	默认设置
作为操作系统的一部分	允许像验证用户一样验证一个进程，并因此获得与用户访问资源一样的访问权限。只有低级身份验证服务才要求这项特权。注意，潜在的访问可能不受默认情况下用户关联的限制，调用进程可能要求将其他任何访问权限添加到访问令牌中。调用进程也可能创建不提供主要标识（用于审核日志中跟踪事件）的访问令牌 要求这项特权的进程应该使用已经包括此特权的本地系统帐户，而不应该使用特别指定此特权的个别用户帐户	未授予任何用户帐户
将工作站添加到域	允许用户将计算机添加到特定的域。要使该特权生效，必须将其作为该域中“默认域控制器策略”的组成部分而分配给用户。具有该特权的用户可以向域中添加最多十个工作站 也可以允许用户将计算机加入域中，其方式是在 Active Directory 中的部门或计算机容器里授予这些用户“创建计算机对象”的权限。具有“创建计算机对象”权限的用户可以向域中添加任意数量的计算机，而不管其是否被分配了“将工作站添加到域”的特权	未授予任何用户帐户
调整处理的内存配额	确定哪个帐户可以使用具有“写入属性”的进程访问另一个进程以此增加分配给另一进程的处理器配额 该用户权限在默认域控制器“组策略”对象（GPO）和工作站及服务器的本地安全策略中定义	管理员
备份文件和目录	允许用户绕过文件和目录权限来备份系统。仅当应用程序试图通过 NTFS 备份应用程序编程接口（API）访问时，才选用该特权。否则，应用正常的文件和目录权限	管理员和备份操作员
忽略遍历检查	浏览任何 NTFS 文件系统或注册表中的对象路径时，允许用户遍历用户无权访问的目录。此特权不允许用户列出目录的内容，只能遍历目录 在域控制器上，将该特权分配给管理员、经过验证的用户和每个人	管理员、备份操作员、高级用户、用户以及成员服务器和工作站上的每个人

（续表）

特权	说明	默认设置
更改系统时间	允许用户设置计算机内部时钟的时间 在域控制器上，将该特权分配给管理员、服务器操作员、Local Service 和 Network Service	管理员、高级用户、Local Service 以及成员服务器和工作站上的 Network ervice
创建令牌对象	当进程使用 NtCreateToken()或其他令牌创建 API 时，允许进程创建可用于访问所有本地资源的令牌 建议需要此特权的进程使用已经包括此特权的本地系统帐户，而不使用特别指定此特权的个别用户帐户	未授予任何用户帐户
创建页面文件	允许用户创建和更改页面文件的大小。该操作是通过在“系统属性”的“高级”选项卡上的“性能选项”下，指定某一特定驱动器的页面文件大小来完成的	管理员
创建永久共享的对象	允许进程在 Windows XP Professional 对象管理器中创建目录对象。该特权对于可扩展对象名称空间的内核模式组件非常有用。以内核模式运行的组件本身就具有该特权，因此无需对其分配该特权	未授予任何用户帐户
调试程序	允许用户向任意进程附加调试程序。此特权对敏感和关键的操作系统组件提供强大的访问	管理员
使计算机和用户帐户成为受信任的以便委派其他帐户	允许用户更改 Active Directory 中用户或计算机对象上的“可委派其他帐户”设置。授予此特权的用户或计算机也必须具有对对象上的帐户控制标志进行写访问的权限。验证委派是由多层客户机/服务器应用程序所使用的一项功能。允许前端服务将正在接收验证的客户凭证用于后端服务。要做到这一点，客户机和服务器必须同时以可委派其他帐户方式运行。误用此特权或误用可委派其他帐户设置会使网络容易受到系统上复杂进攻的破坏，如使用特洛伊木马程序模仿传入的客户并使用它们的凭据访问网络资源 该特权不授予成员服务器或工作站上的任何人，因为这种授权无任何意义	在域控制器上，该特权默认情况下授予管理员
从远程系统强制地关机	允许用户从网络上的远程位置关闭计算机。参阅关闭系统特权 在域控制器上，该特权分配给管理员和服务器操作员	成员服务器和工作站上的管理员
生成安全审核	允许进程在安全日志中创建记录。安全日志用于跟踪未经授权的系统访问；参阅特权“管理审核和安全日志”	Local Service 和 Network Service
增加调度优先级	允许具有“写”属性的进程访问其他进程以便增加其他进程的执行优先级；具有该特权的用户可以更改“任务管理器”中某个过程的调度优先级	管理员
加载和卸载设备驱动程序	允许用户安装和卸载即插即用的设备驱动程序。该特权对安装非即插即用设备的驱动程序没有影响。只有系统管理员才可以安装非即插即用设备 建议不要将此特权授予任何其他用户。设备驱动程序以受信任（或高级特权）程序运行。具有加载和卸载设备驱动程序特权的用户，可能会由于将恶意代码误当作设备驱动程序安装而无意误用该特权。因此建议管理员要提高警惕，且只安装带有经验证的数字签名证书的驱动程序	管理员

（续表）

特权	说明	默认设置
锁定内存中的页面	允许进程将数据保存在物理内存中，以防系统将分页数据，写到磁盘上的虚拟内存中。分配该特权可能致使系统性能严重降低 某些系统进程本身就具有该特权	未分配给任何人
管理审核和安全日志	允许用户指定文件、Active Directory 对象和注册表项之类的单个资源的对象访问审核选项。只有当启用了“审核策略”中的对象访问审核后，才可以真正执行对象访问审核操作。具有此特权的用户还可以从事件查看器中，查看并清除安全日志 具有此特权的用户还可以从事件查看器中查看并清除安全日志	管理员
修改固件环境值	允许通过 API 的某个进程或通过“系统属性”的某个用户来修改系统环境变量	管理员
图示单个进程	允许用户运行 Windows XP Professional 性能监视工具来监视非系统进程的性能 在域控制器上，仅将该特权分配给管理员	成员服务器和工作站上的管理员和高级用户
配置文件系统性能	允许用户运行性能监视工具监视系统进程的性能	管理员
从插接站删除计算机	允许便携式计算机用户通过单击“开始”→“弹出 PC”来脱开计算机	管理员、高级用户和用户
替换进程级令牌	确定哪个用户帐户可以初始化一个进程，以取代与已启动的子进程相关的默认令牌 该用户权限在“默认域控制器组策略”对象和工作站及服务器的本地安全策略中进行定义	本地服务和网络服务
还原文件和目录	还原备份的文件和目录时，允许用户绕过文件和目录权限，并将任何有效的安全主体设为对象的所有者。参阅“备份文件和目录”特权	管理员和备份操作员
关闭系统	允许用户关闭本地计算机 在成员服务器上，该权利授予管理员、高级用户和备份操作员 在域控制器上，该权利授予管理员、帐户操作员、备份操作员、打印操作员和服务器操作员	管理员、备份操作员、高级用户和工作站用户
同步目录服务数据	允许进程提供目录同步服务。该特权仅对域控制器有效	未授予任何用户帐户
获得文件或其他对象的所有权	允许用户获得系统中任何可得到的对象的所有权，包括 Active Directory 对象、NTFS 文件和文件夹、打印机、注册表项、进程和线程	管理员

某些特权可以覆盖在对象上设置的原有权限。例如，用户作为备份操作员组的成员登录到域时，具有对所有域服务器执行备份操作的权利。但是，该操作同时还要求用户能够读取这些服务器上的所有文件，甚至是文件所有者已经明确设置对所有用户（包括备份操作员组成员）都拒绝访问的文件。在这种情况下，执行备份的用户权利优先于所有的文件和目录权限。

2. 赋予用户特权

这里以“将工作站添加到域”权限为例，介绍如何设置用户特权。通过给用户赋予“将工作站添加到域”的权限，可以让用户向一个域中添加最多 10 台计算机。默认情况下，Windows Server 2008 的“域中添加工作站”的权限赋予“Authenticated Users”用户组，即任何授权用户可以添加 10 台计算机到域森林中，是非常危险的，仅将该特权赋予指定帐户即可。

01 以管理员帐户登录域控制器，依次选择“开始”→“管理工具”→“组策略管理”选项，打开“组策略管理”窗口。依次展开“林：coolpen.net”→“域”→“coolpen.net”→“组策略对象”→“Default Domain Controllers Policy（默认域控制器策略）”选项，如图 5.29 所示。

02 右击“Default Domain Controllers Policy”并选择快捷菜单中的“编辑”选项，打开“组策略管理编辑器”窗口。依次展开“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“本地策略”→“用户权限分配”选项，如图 5.30 所示。

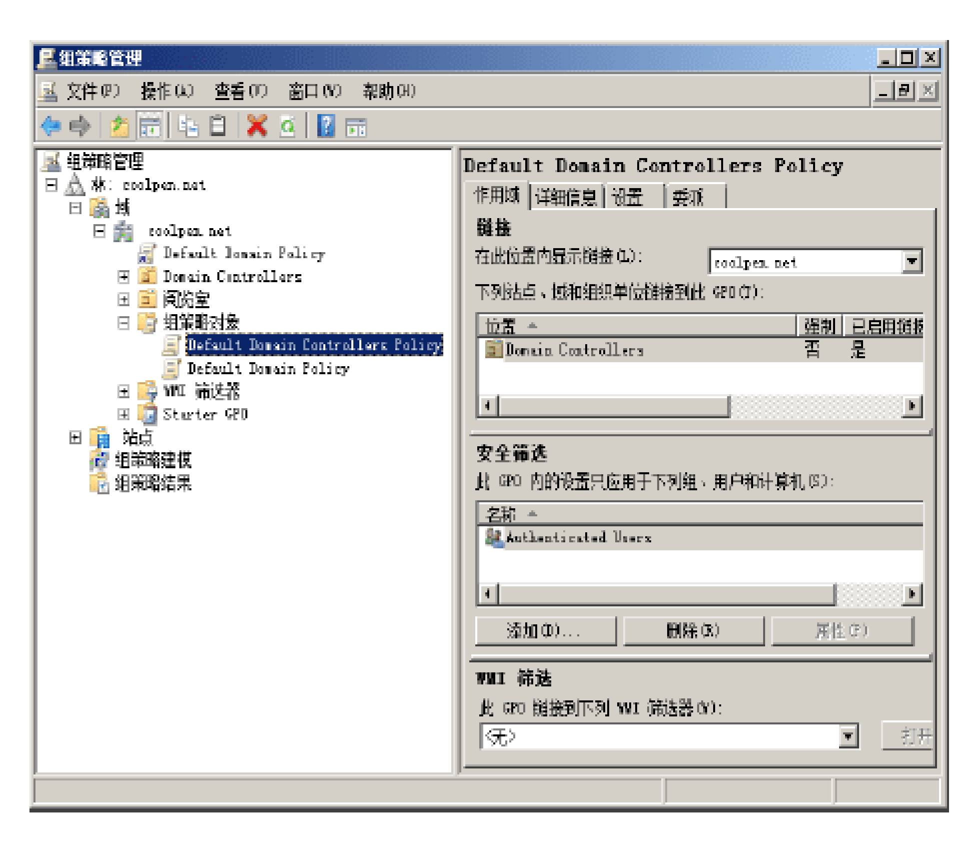


图 5.29　“组策略管理”窗口

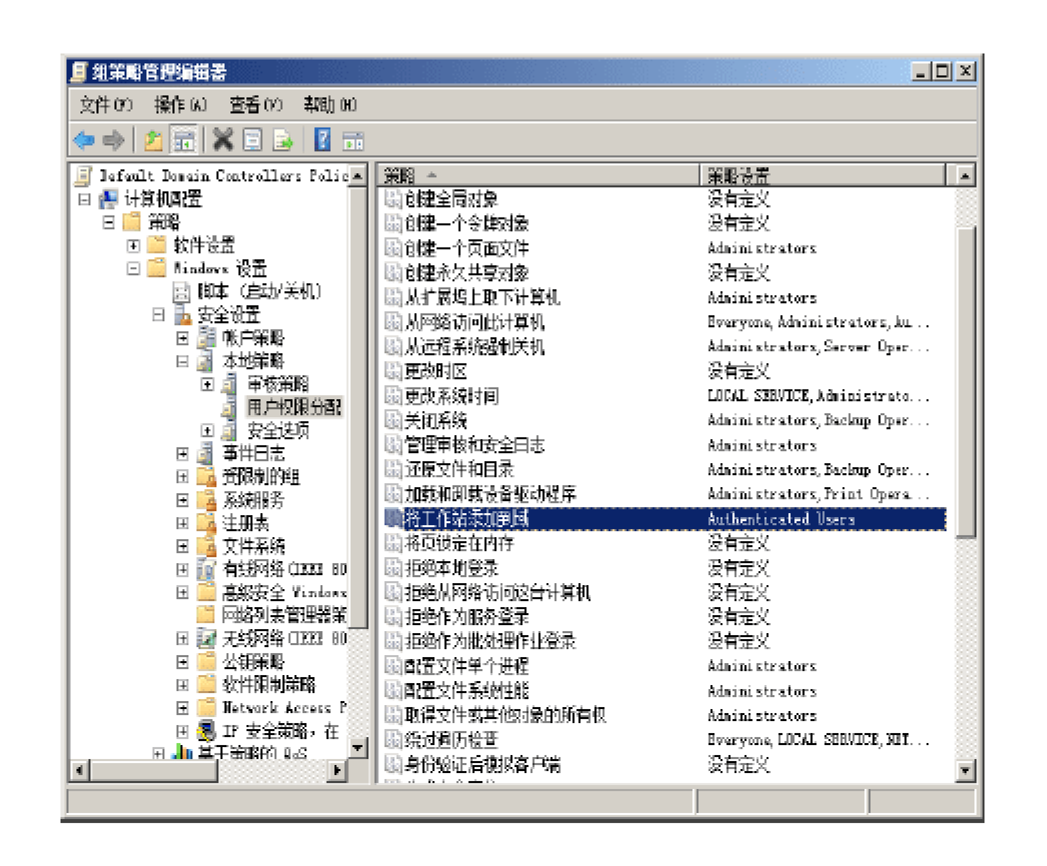


图 5.30　“组策略管理编辑器”窗口

03 双击“将工作站添加到域”策略，显示“将工作站添加到域 属性”对话框。默认情况下，列表中只有“Authenticated Users”用户组，即所有授权用户都拥有该特权，选择该帐户并单击“删除”按钮，即可将其删除。单击“添加用户或组”按钮，显示“添加用户或组”对话框。单击“浏览”按钮，显示“选择用户、计算机或组”对话框，在“输入对象名称来选择”文本框中，输入用户帐户名 liuxh。如图 5.31 所示。

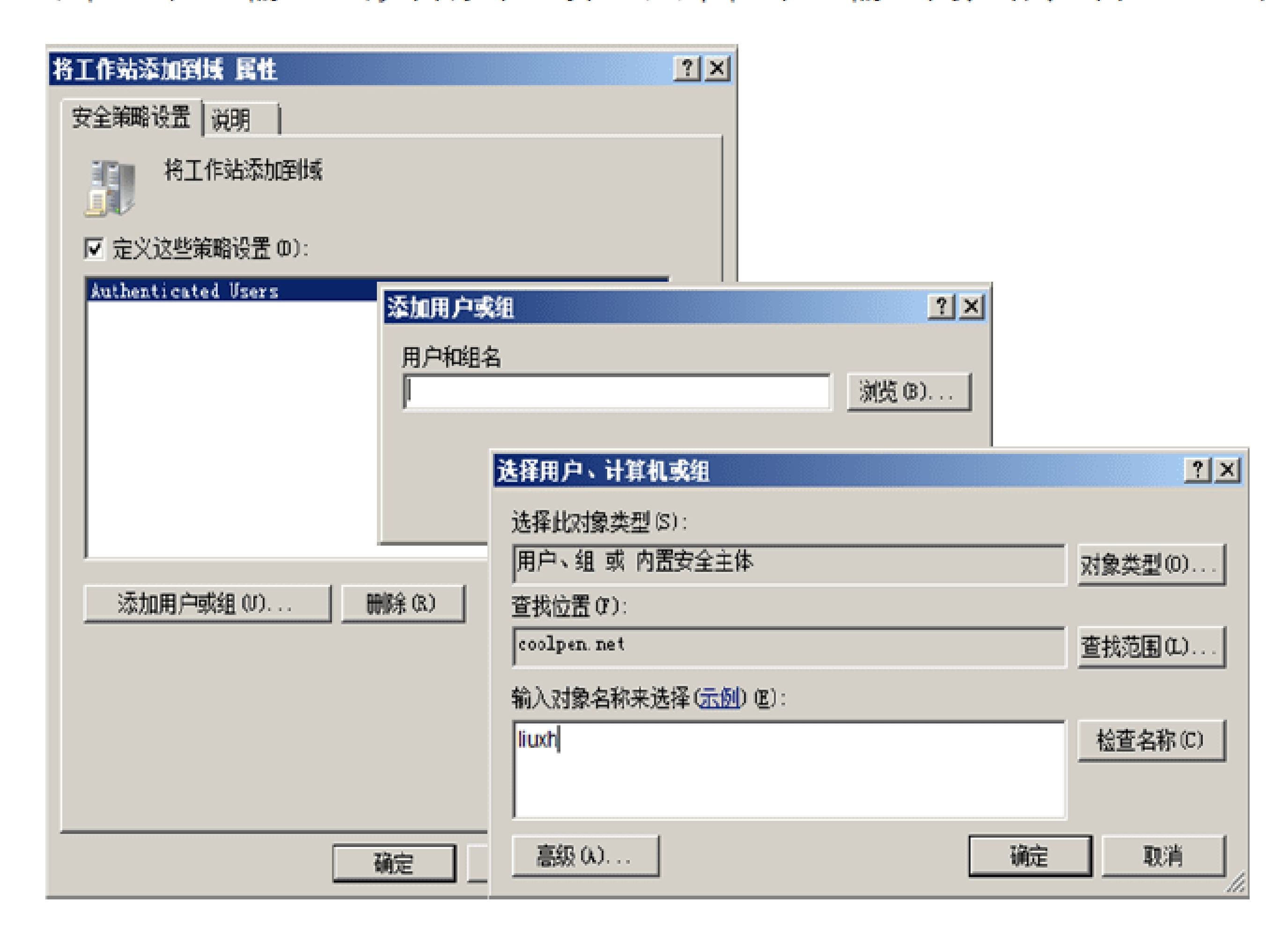


图 5.31　将工作站添加到域

04 依次单击“确定”按钮，保存设置即可。当客户端需要添加到域时，使用“liuxh”帐户，并输入相应的密码即可完成用户的添加。

5.4.2 用户登录权利

登录权利，是指分配给用户，并指定用户以哪种方式登录系统的用户帐户权利。

1. 默认登录权利

默认的登录权利如表 5.2 所示。

表 5.2 默认的登录权利

登录权利	说明	默认设置
从网络访问计算机	允许用户通过网络连接到计算机	管理员、每个人、用户、高级用户和备份操作员
允许通过终端服务登录	允许用户通过远程桌面连接登录到本计算机	管理员和远程桌面用户
作为批处理作业登录	允许用户使用批处理查询工具登录 如果安装了 Internet 信息服务（IIS），则系统将该权利自动分配给匿名访问 IIS 的内置帐户	没有任何用户帐户
作为服务登录	允许某种安全原则以服务身份登录。可以将服务配置为在 Local System、Local Service 或 Network Service 帐户下运行，这些帐户具有作为服务登录的内置权利。在单个帐户下运行的任意服务都必须授予该权利	没有任何用户帐户
本地登录	允许用户通过计算机键盘登录	管理员、高级用户、用户、来宾和备份操作员
作为服务登录	允许某种安全原则以服务身份登录。可以将服务配置为在 Local System、Local Service 或 Network Service 帐户下运行，这些帐户具有作为服务登录的内置权利。在单个帐户下运行的任意服务都必须授予该权利	没有任何用户帐户
拒绝从网络访问这台计算机	禁止用户或组从网络连接到本计算机	没有任何用户帐户
拒绝本地登录	禁止用户或组直接通过键盘登录	没有任何用户帐户
拒绝作为批处理作业登录	禁止用户或组通过批处理队列工具登录	没有任何用户帐户
拒绝作为服务登录	禁止用户或组作为服务登录	没有任何用户帐户
拒绝通过终端服务登录	禁止用户或组作为终端服务客户登录	没有任何用户帐户

2. 赋予用户远程登录权利

远程登录权利允许用户和组，通过网络远程连接到域控制器，如借助微软控制台或其他方式等。在 Windows Server 2008 域控制器上，系统默认将该权限赋予 Administrators、Authenticated Users、Everyone、ENTERPRISE DOMAIN CONTROLLERS 和 Pre-Windows 2000 Compatible

Access 等组。可以使用如下方法重新设置，另外，“终端服务”不受此用户权利影响。

01 以管理员帐户登录域控制器，打开“Default Domain Controllers Policy”策略的“组策略管理编辑器”窗口。依次展开“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“本地策略”→“用户权限分配”选项，找到“从网络访问此计算机”策略，如图 5.32 所示。

02 双击“从网络访问此计算机”策略，显示如图 5.33 所示的“从网络访问此计算机 属性”对话框。建议仅保留 Authenticated Users 组，即只赋予授权的用户帐户此权限。

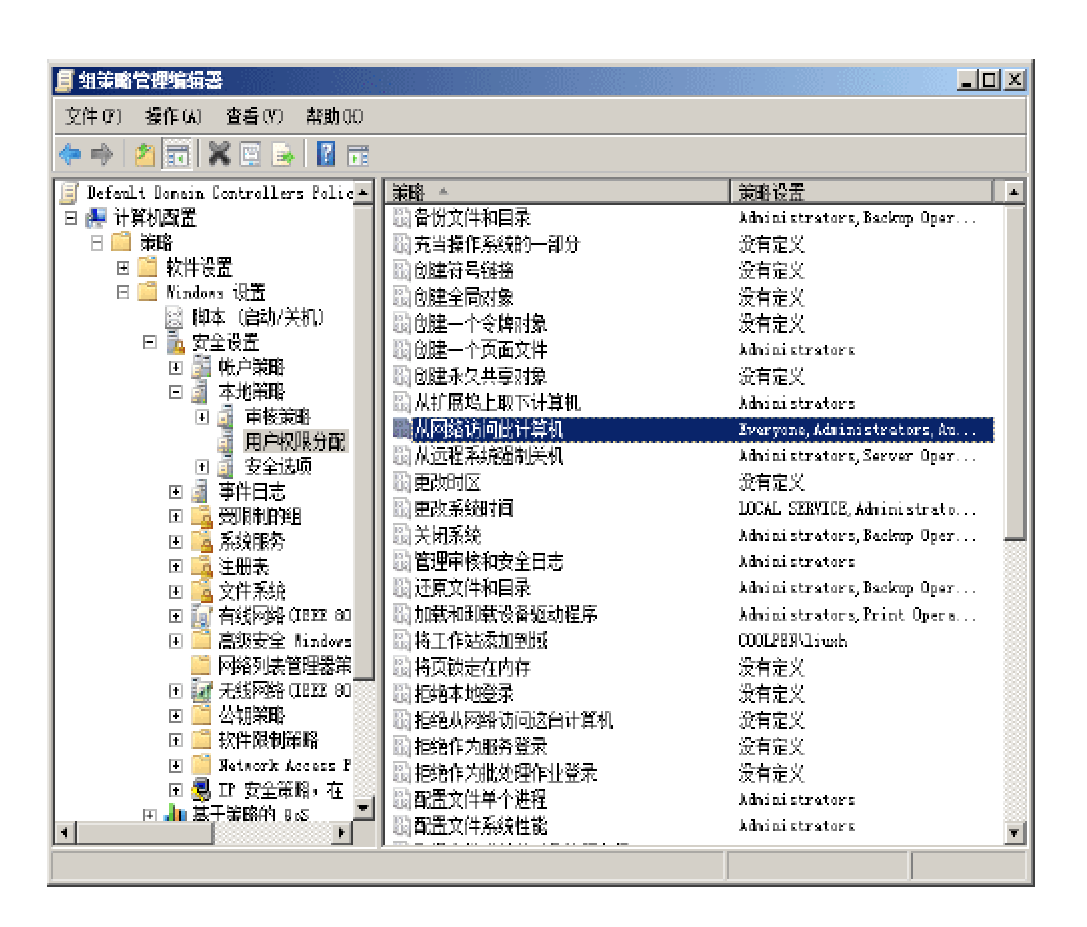


图 5.32 “组策略管理编辑器”窗口

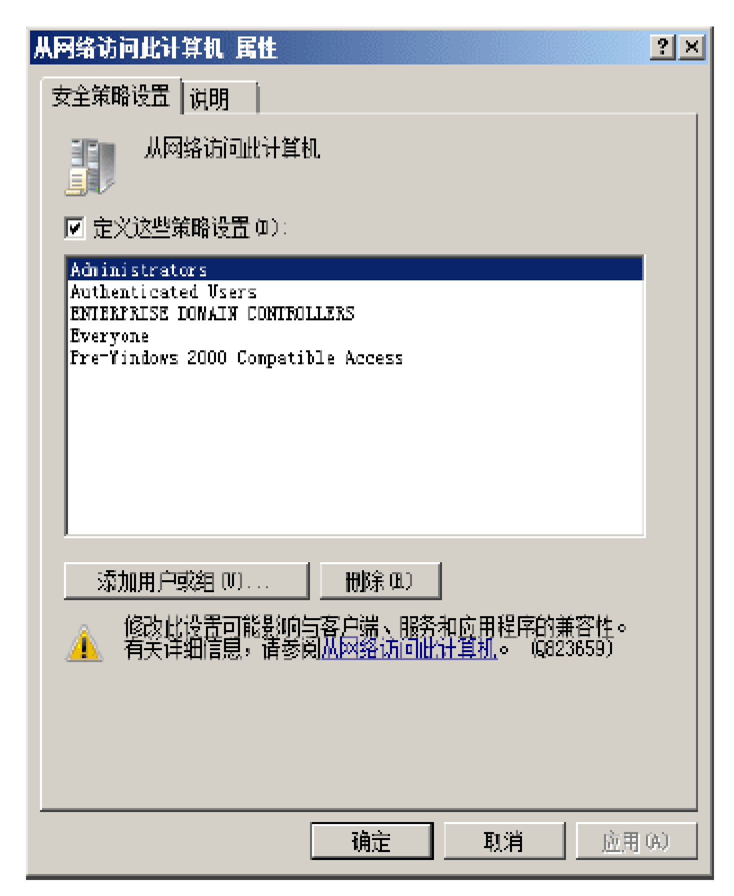


图 5.33 “从网络访问此计算机属性”对话框

03 如果还需要将此权限赋予其他用户帐户，可以单击“添加”按钮，将其添加到列表中，与赋予拥护特权的操作完全相同，此处不复赘述。



注意 在工作站和独立服务器上，默认情况下，该登录权利被赋予 Administrators、BackupOperators、PowerUsers、Users 和 Everyone 组。

5.4.3 将用户权利指派到组

为避免权限管理混乱，应尽量将用户权利指派到组，然后将需要获得此权限的用户添加到该组中，尤其是对于用户较多的域网络，更应如此。如果是 Windows Server 2008 域网络，则可以在域控制器的“组策略管理”工具中，编辑域控制器的默认策略“Default Domain Controllers Policy”或者“本地安全策略”中的相关设置。如果是独立服务器，只能在“本地安全策略”中完成。

01 在 Windows Server 2008 域控制器上，依次选择“开始”→“管理工具”→“本地安全策略”选项，打开“本地安全策略”窗口。

02 依次展开“安全设置”→“本地策略”→“用户权限分配”选项，在右侧窗口中列出了可以分配给用户的所有用户权限，如图 5.34 所示。

03 双击要分配给组的权限，打开属性对话框，添加要指派给的组名即可。例如，双击“从网络访问此计算机”策略，显示如图 5.35 所示“从网络访问此计算机 属性”对话框。从列表中显示具备此权利的用户或者组。

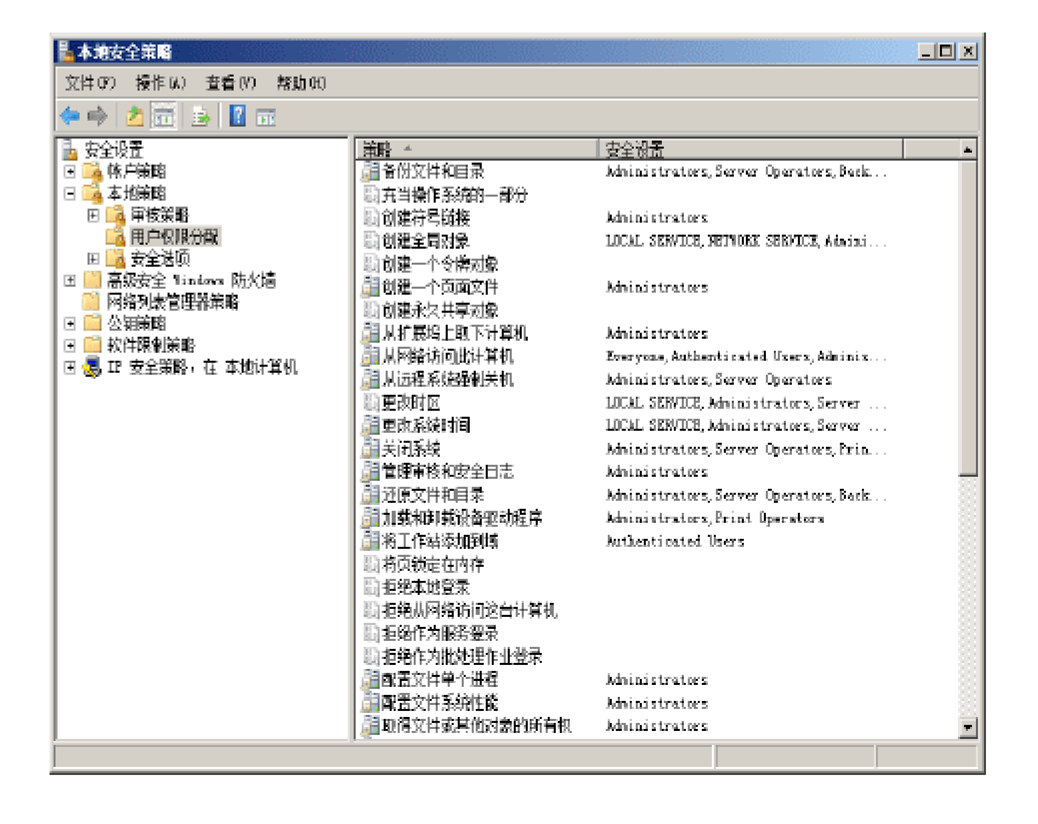


图 5.34 “用户权限分配”窗口

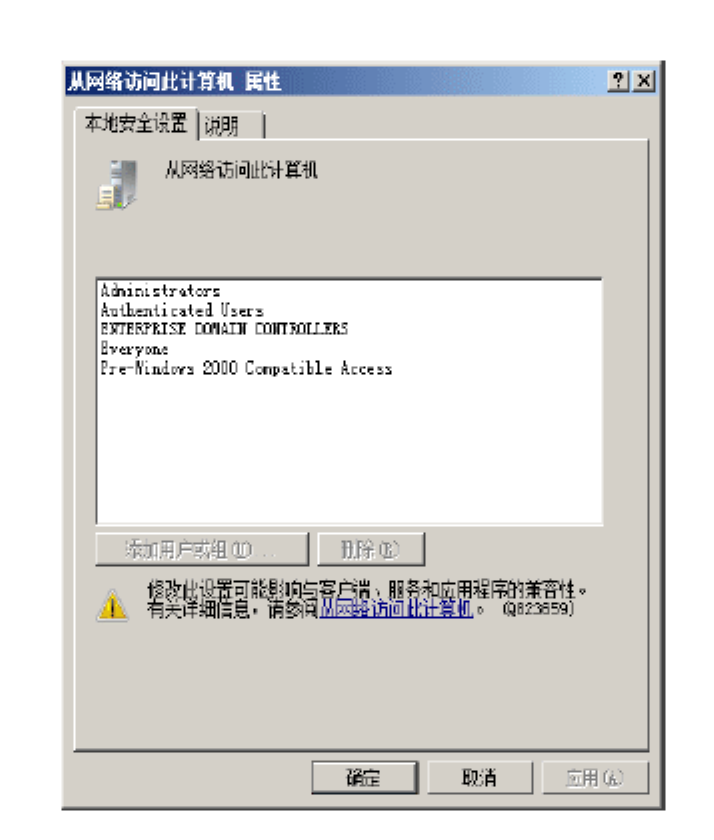


图 5.35 “从网络访问此计算机 属性”对话框

当为组分配了某个权限以后，该组中的用户同时也会拥有该权限，而以后向该组中添加用户时，新用户也会拥有此权限。

通常情况下，可参考如下说明将适当地权限分配相应的用户组：

- 管理员组（Administrators）可以被授权的权利包括更改系统事件、创建页面文件、装载和卸载设备驱动程序、在本地登录、管理审核安全日志、配置单一进程、配置系统性能、关闭系统、取得文件或者对象的所有权；
- 备份操作员组（Backup Operators）可以被授权的权利包括备份文件和目录、在本地登录、还原文件和目录（如果不想让备份操作员组具备还原文件和目录的权利，可以重建一个新的用户组）；
- 用户组可以被授权的权利为在本地登录（默认的）；
- 将有关“Everyone”组的权利删除。尤其是在 Windows 2000 系统中，默认情况下，Everyone 组被赋予“完全控制”权限，毫无疑问，对系统安全而言，这是非常危险的；
- 将有关“Power Users”组的权利删除。

不授予任何权利，除非应用程序有特殊的要求，必须取消其他所有默认状况下的权利设定。

5.5 用户帐户控制

通常情况下，Windows 的很多用户都拥有管理特权，对计算机安全管理存在很大的隐患。在 Windows Vista 和 Windows Server 2008 中，UAC（User Account Control，用户帐户控制）体现了最小特权原则，即在执行任务时使用尽可能少的特权。配置用户帐户控制将涉及到除内建管理员帐户之外的所有交互用户，所以操作过程中，既需要对核心操作系统做一定程度的改变，还必须改变默认用户桌面的工业标准，以及通过独立软件供应商（Independent Software Vendor，ISV）推广默认用户最优化方案的应用。

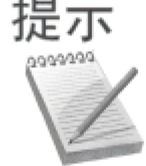
5.5.1　用户帐户控制概述

在 Windows Server 2008 系统中，UAC 主要涉及的是客户端功能。对于系统管理员而言，Windows Server 2008 中的 UAC，主要是使用组策略来管理 Windows Vista 客户端的 UAC 策略。UAC 适用于 Windows Vista 的所有版本。

UAC 允许用户验证系统行为，从而阻止未经认证的计算机系统的变动。当用户以管理员身份登录到 Windows Vista 和 Windows Server 2008 时，会得到两个访问令牌：一是完全访问令牌，二是标准受限访问令牌。

标准受限访问令牌对受限进程没有管理特权，并且禁用管理员组 SID，主要用于启动 Windows 资源管理器（explorer.exe）和所有的子进程。所有应用程序默认都是以标准用户令牌运行的，除非管理员授予其权限，否则不能以完全访问令牌运行。注意，由于应用程序将继承父进程的特权级别，因此，如果父进程以完全访问令牌运行，则子进程也会继承其特权级别，且不会提示管理员。例如，以管理员身份运行命令提示符，则在命令提示符下运行的所有进程，都将具备管理员特权。

提示



Explorer.exe 默认是非提升权限的，所以，当右击执行“以管理员身份运行”命令时，会重新启动一个与原窗口同样的窗口。管理员可以借助相关工具，在每个文件夹的右键快捷菜单中添加一个“Elevate Explorer Here”命令。这样，就可以随时随地启动一个提升了权限的 Windows Explorer 了。Explorer.exe 进程并不是系统运行时所必需的，所以，可以用任务管理器来结束它，并不影响系统的正常工作。

5.5.2　UAC 提升用户体验

UAC 对用户体验的影响，在本地管理员组（Local Administrators group）的成员上体现得最为显著。普通用户无需注销也能执行管理任务，其提示窗口与管理员是一样的，只是需要输入密码而已。

1. 凭据提示

在 Windows Vista 和 Windows Server 2008 中，除内置管理员（Built-in Administrator）外，所有用户都将以普通用户身份运行程序。如果某项任务需要管理员权限，就会显示提升凭据提示，如图 5.36 所示。此时，用户需要输入一个有效的用户名和密码来证明自己是授权用户。

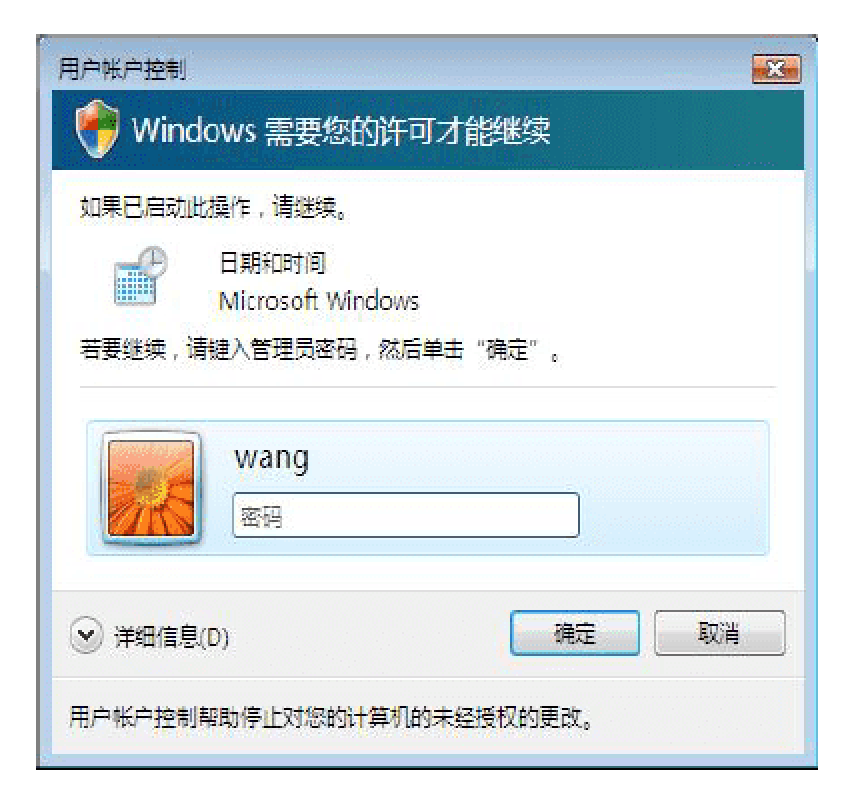


图 5.36　普通用户试图执行管理任务时会显示凭据提示

2. 确认提示

如果本地计算机的 UAC 设置为“管理批准模式（Admin Approval Mode）”，则当管理员组

的成员需要以管理员权限执行任务时，就会出现如图5.37所示确认提示。



图 5.37　管理员试图执行管理任务时会显示同意提示

为了让用户能够更好地做出决定，UAC 权限提升提示使用背景颜色、盾牌图标样式和提示信息来表示不同程度的潜在安全风险。

应用程序尝试使用管理员的完全存取令牌运行时，Windows Vista 和 Windows Server 2008 会分析可执行文件以确定其发行者，并使用此信息来决定正确的用户体验。例如，如果提示信息背景颜色为灰色（如图 5.38 所示），则表明需要管理权限的应用程序是通过代码验证签名的，且属于本地计算机的信任程序，如 Microsoft 防火墙客户端（Microsoft Firewall Client）和 ISA（Internet Security and Acceleration Server）服务器。

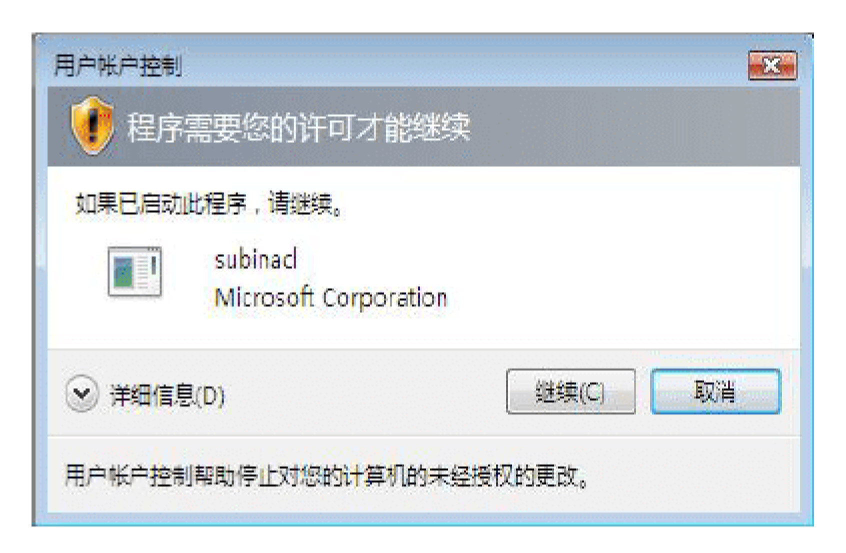


图 5.38　应用程序已由代码验证签名且受本地计算机信任

如果提示信息背景颜色为黄色（如图 5.39 所示），表明需要管理权限的应用程序不具有正确代码验证签名，因此运行它是有一定风险的。

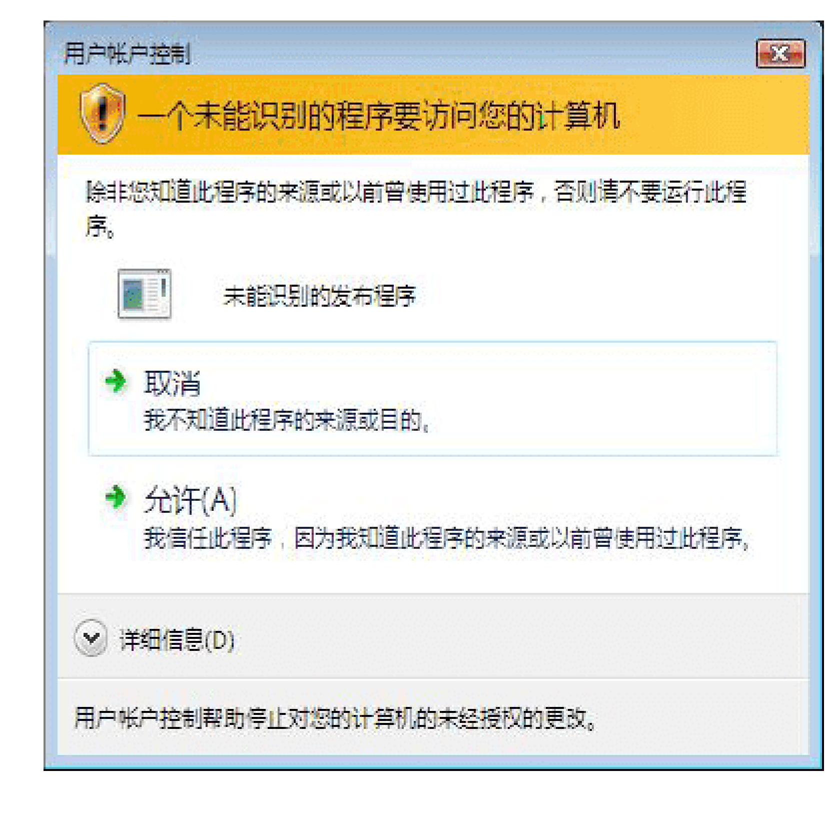


图 5.39　应用程序未经签名时的提示信息

如果提示信息背景颜色为红色（如图 5.40 所示），并且盾牌图标也变为“红底白叉号”，则表明需要管理权限的应用程序来自被阻止或是非受信任的发布者。管理员可以将发布者签名证书存放在本地计算机的非受信任证书库中，以便阻止特定的发布者，当然，也可以使用组策略来达到同样的目的。

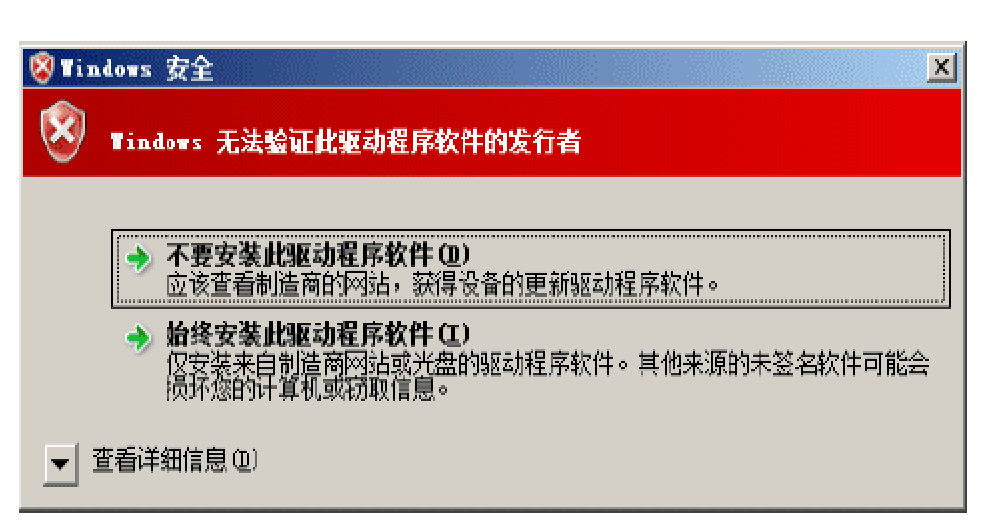


图 5.40　阻止特定的发布者

注意  UAC 对话框会根据发布者的代码验证签名信任级别，来决定其所显示的细节信息，包括可执行名称和路径。

在 Windows Vista 和 Windows Server 2008 中，如图 5.41 所示的盾牌图标表明，当用户执行受保护的操作或是程序时，UAC 会提示验证。

某些控制面板组件配置窗口中会显示 UAC 提示验证图标，例如，如图 5.42 所示“日期和时间”对话框。默认用户可以查看时钟和更改时区，而要更改本地系统时间，则需要完全管理员访问令牌。原因很简单，如果用户更改了系统时间，那么，将导致事件日志中的事件混乱，或者将影响计算机访问 Windows 域时的验证。

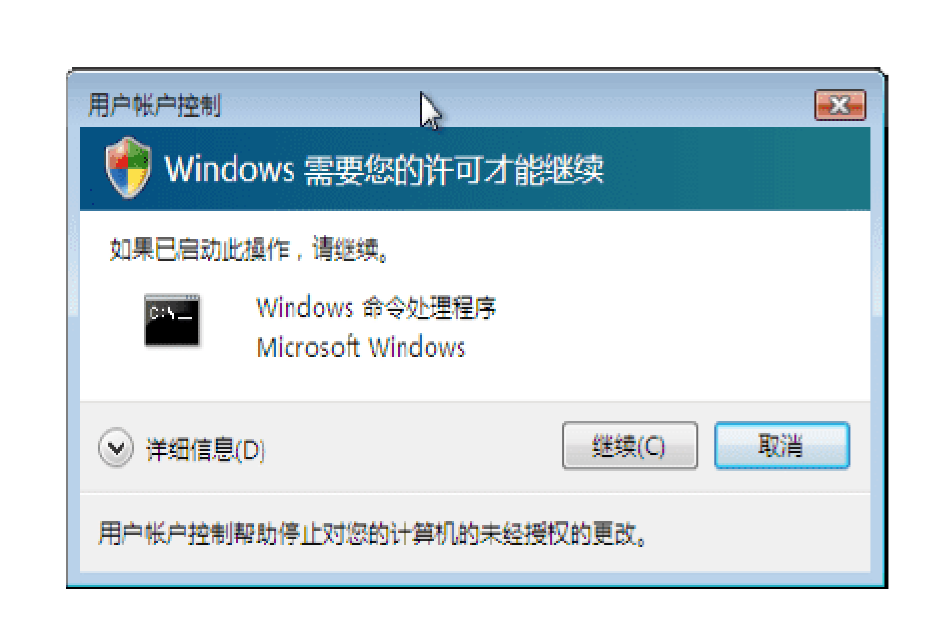


图 5.41　UAC 提示验证图标表示

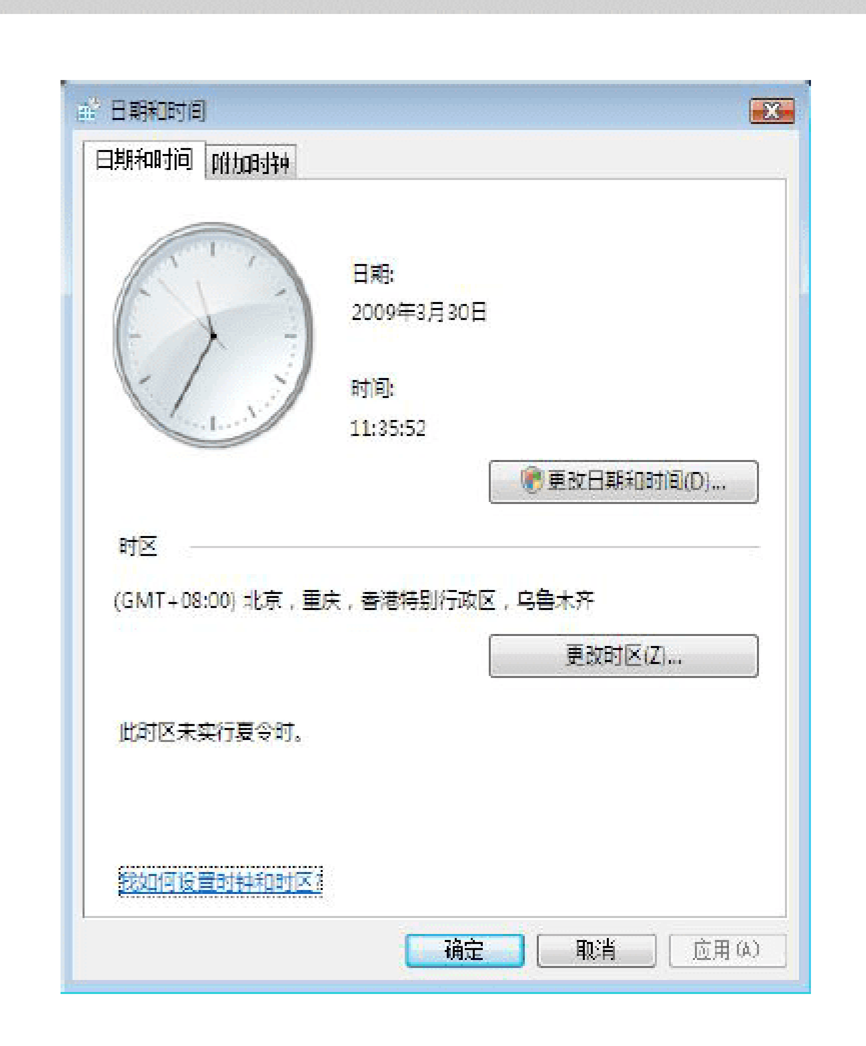


图 5.42　“日期和时间”对话框

5.5.3　创建 UAC 组策略

管理员可以在域控制器的“组策略管理编辑器”窗口中，或者“本地安全策略”编辑器窗口中，查看和编辑 UAC 相关的组策略。依次展开 “本地计算机策略”→“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“安全选项”分支，其中与 UAC 相关的策略包括 10 条，如图 5.43 所示。

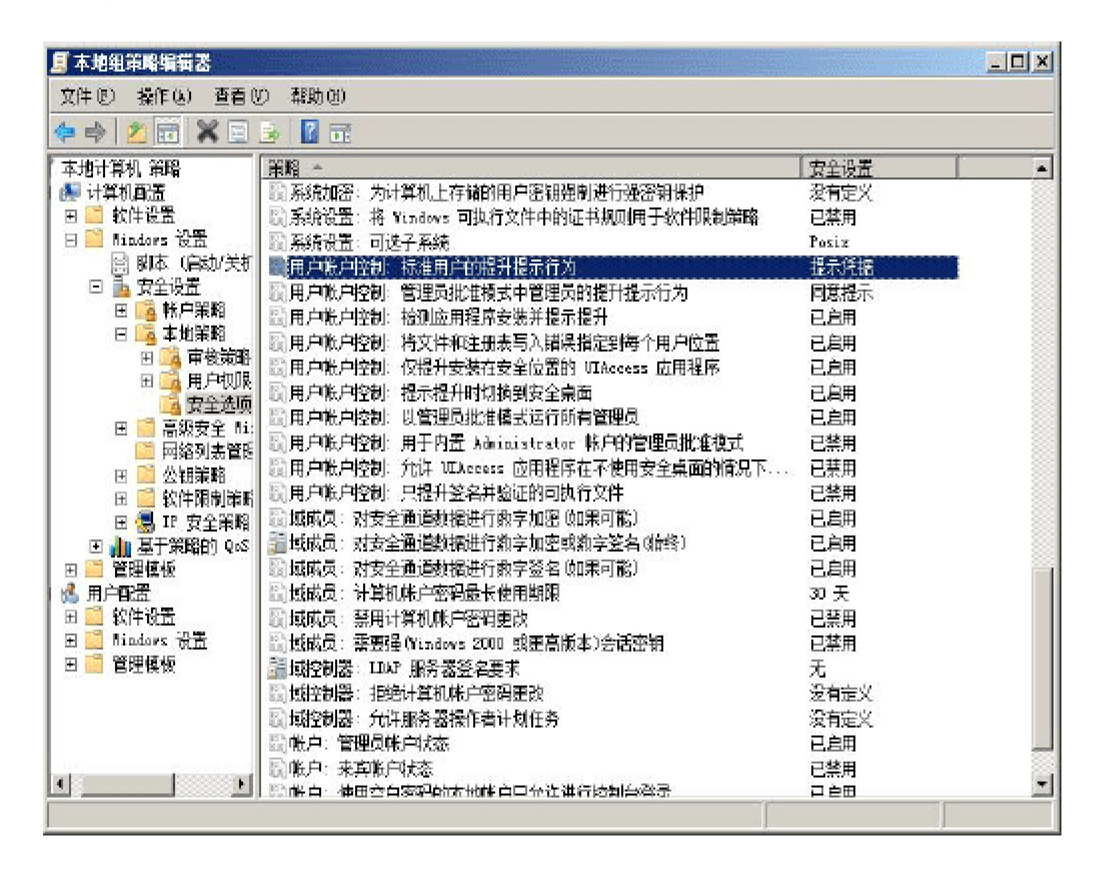


图 5.43　“本地组策略编辑器”窗口

Windows Server 2008 域策略和 Windows Server 2008 或 Vista 系统的本地组策略的默认设置是有所不同的，本例中以本地组策略为例介绍的。

1. 用户帐户控制：标准用户的提升提示行为

UAC 提供了灵活的权限提升提示体验，如果用户能够提供合法的管理员名和密码，则权限提升操作成功。如果不想赋予用户提升的权限，可以将此设置设为自动拒绝提升请求。默认此设置为“提示凭据”。双击“用户帐户控制：标准用户的提升提示行为”策略，显示如图 5.44 所示对话框，在下拉列表中选择希望应用的提示行为即可。

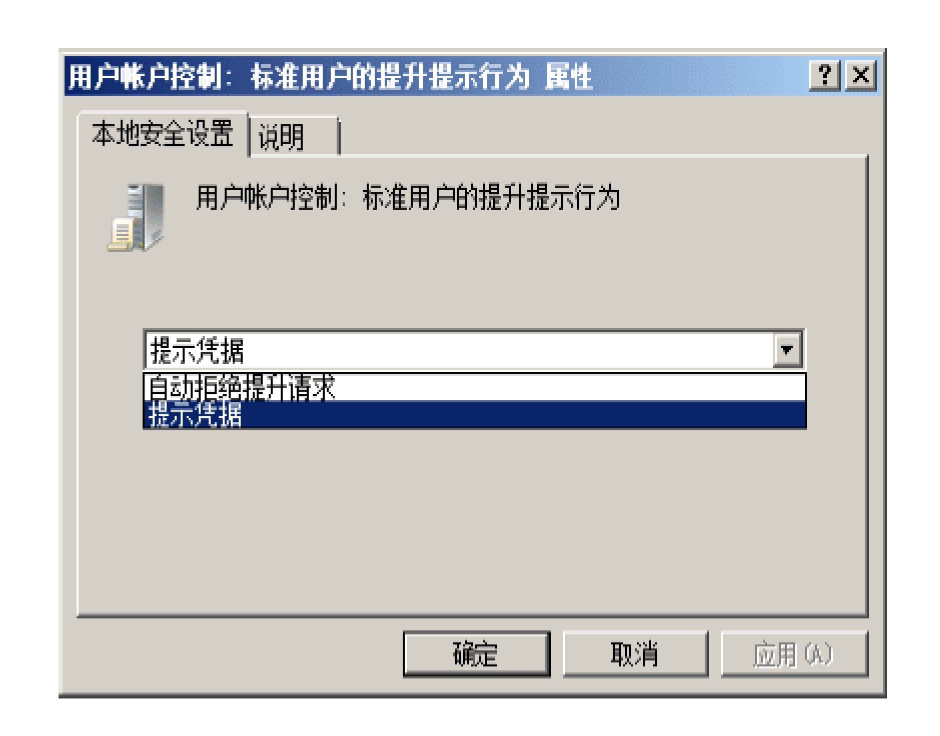


图 5.44 “用户帐户控制：标准用户的提升提示行为 属性”对话框

2. 用户帐户控制：管理员批准模式中管理员的提升提示行为

如果某操作需要管理员特权才能运行，此策略会控制管理批准模式下管理员的 UAC 提示体验。虽然默认设置也很方便，但是强制凭证也是必要的。在默认情况下，除了内置管理员帐户外的所有帐户都会在需要提升权限前被提示同意操作。如果用户启用了此项策略，就可以选择要求管理员提供凭据来获得提升权限，或者通过无须提示凭据或同意提示来降低安全性，如图 5.45 所示。

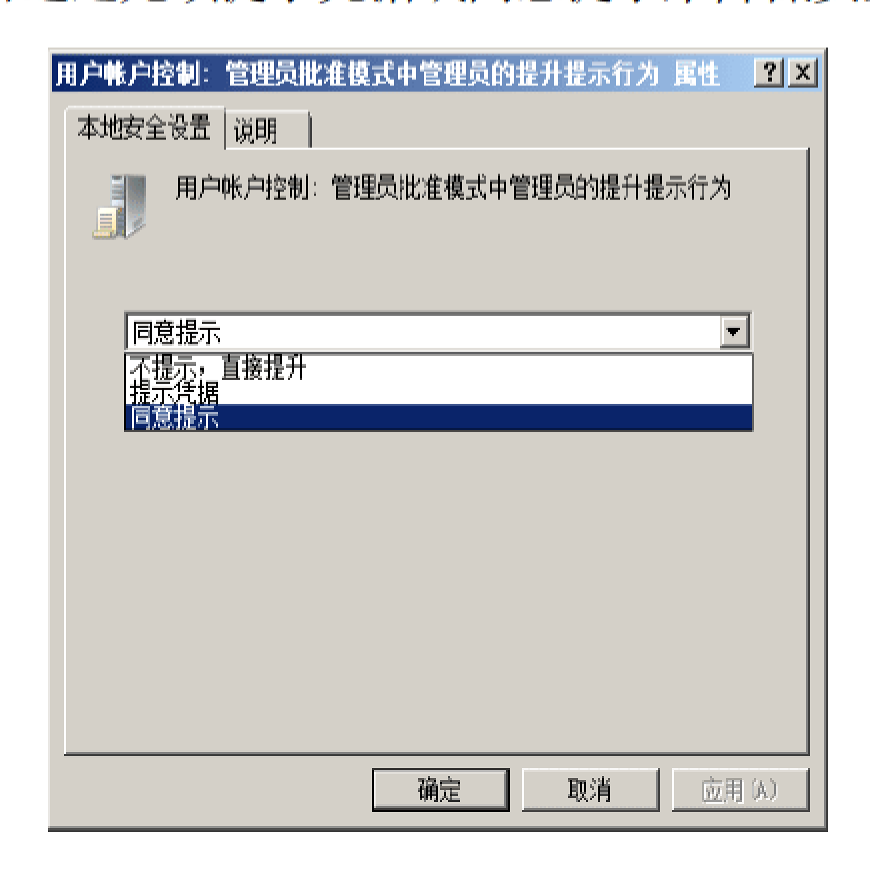


图 5.45 “用户帐户控制：管理员批准模式中管理员的提升提示行为 属性”对话框

3. 用户帐户控制：检测应用程序安装并提示提升

此设置允许或是禁止应用程序安装检测。建议启用此设置（默认启用），如图 5.46 所示。

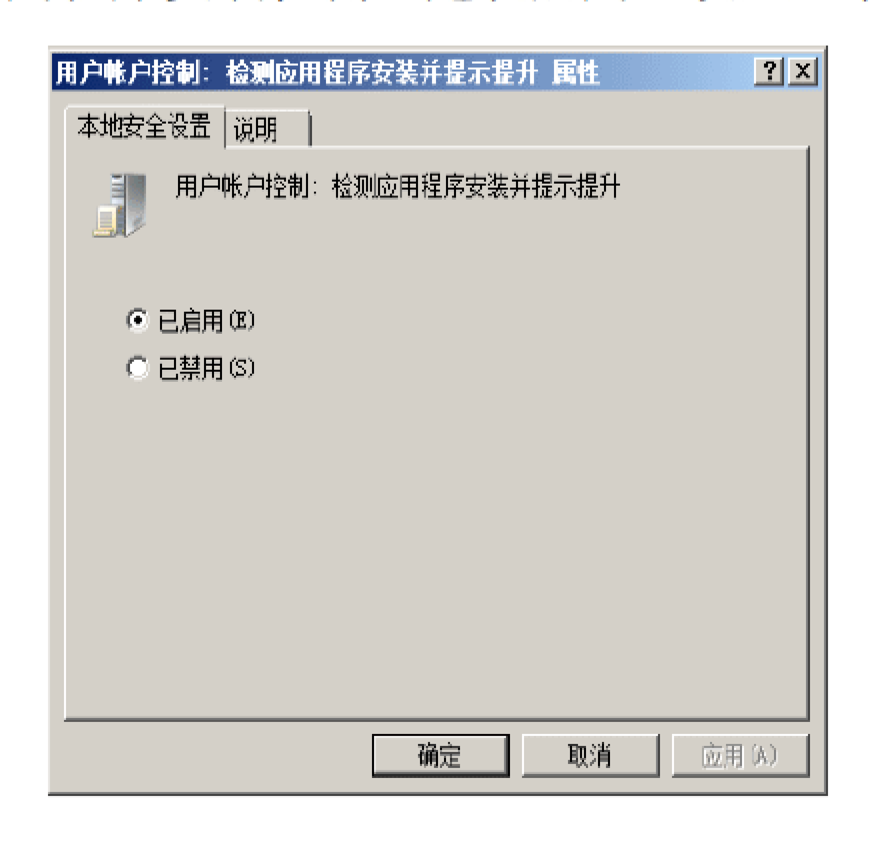


图 5.46 “用户帐户控制：检测应用程序安装并提示提升 属性”对话框

4. 用户帐户控制：将文件和注册表写入错误指定到每个用户位置

此设置允许或是禁止将文件和注册表错误重定向。如果只使用 Windows Vista 或 Windows Server 2008 认证的软件，可以禁用此设置。默认此设置是启用的，如图 5.47 所示。

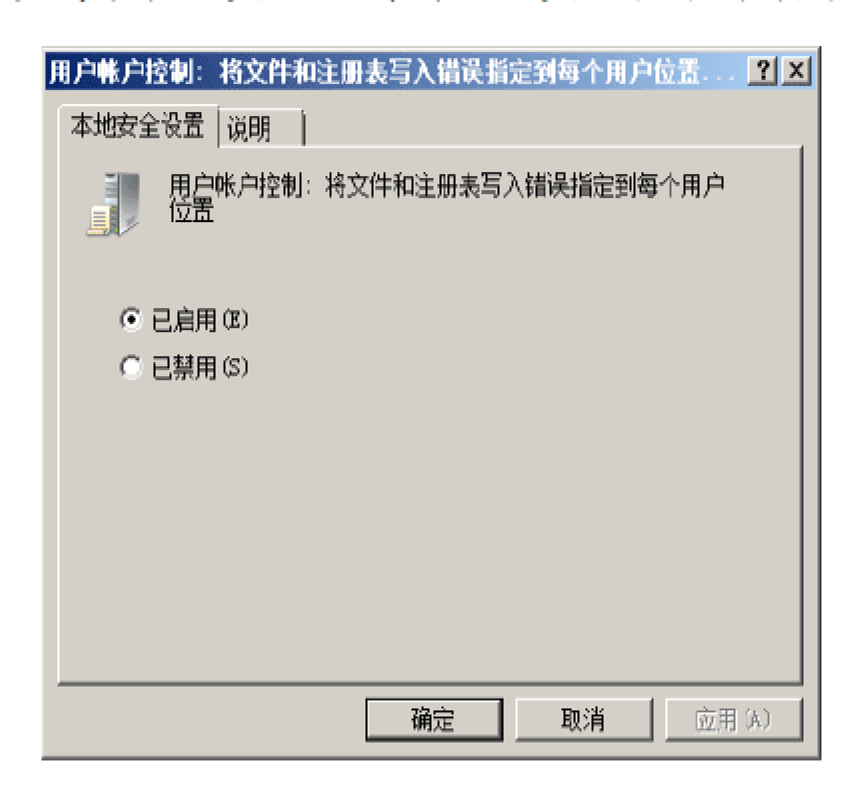


图 5.47　“用户帐户控制：将文件和注册表写入错误指定到每个用户位置 属性”对话框

5. 用户帐户控制：仅提升安装在安全位置的 UIAccess 应用程序

UIAccess 应用程序是与 Windows UAC 提升对话框交互最为频繁的程序，Windows Vista 和 Windows Server 2008 UAC 提升对话框是受到高完整性级别保护的，因此，UIAccess 应用程序必须在程序清单中声明其需求。当程序运行时，UIAccess 会获得特殊的完整性级别交互权限。由于 UIAccess 应用程序功能强大，此设置会强制其从安全目录路径启动。UIAccess 应用程序必须具备合法且信任的代码验证签名。默认此设置是启用的，如图 5.48 所示。

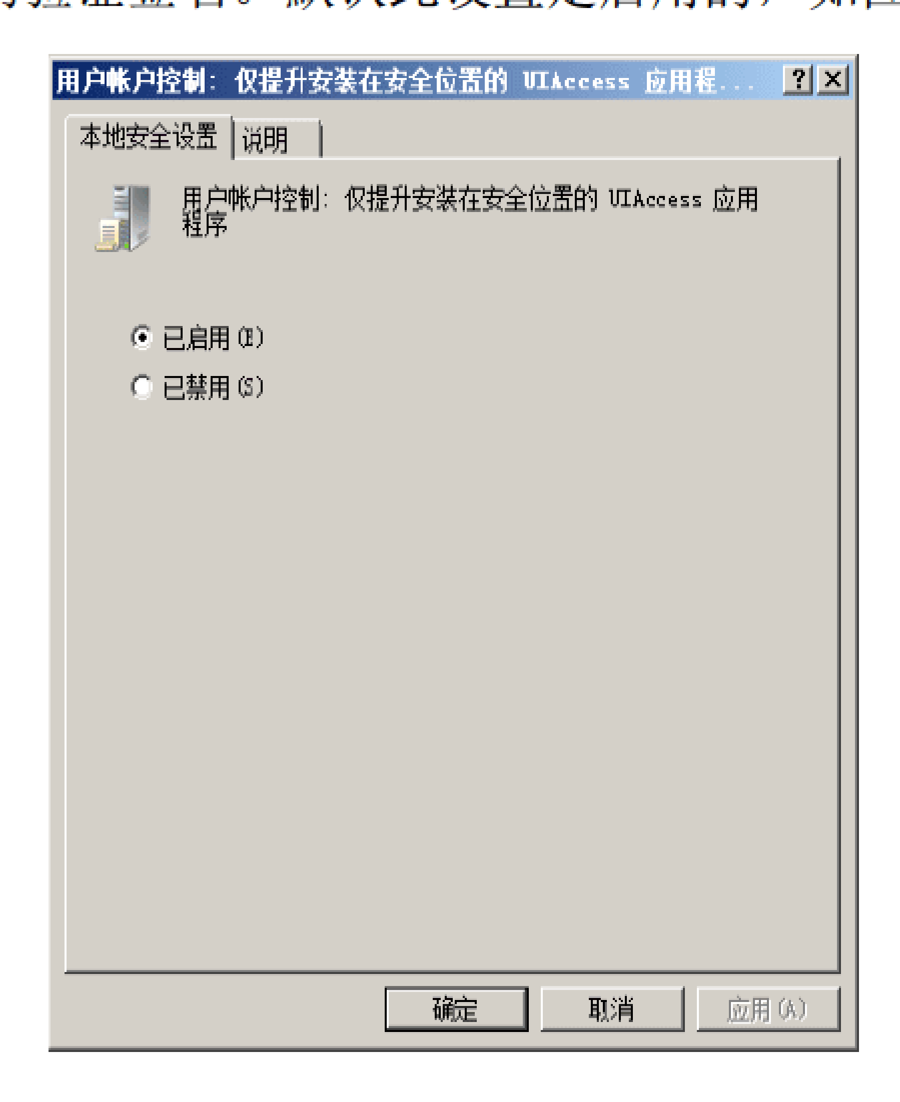


图 5.48　“用户帐户控制：仅提升安装在安全位置的 UIAccess 应用程序 属性”对话框

6. 用户帐户控制：提示提升时切换到安全桌面

此设置用于定义将提升提示显示在用户桌面上还是安全桌面上。安全桌面阻止出站欺骗，也就是说，安全桌面所阻止的信息是无法盗用的。交互用户桌面的 UAC 对话框可以模仿，没有安全桌面的 UAC 对话框保险。默认此设置是启用的，如图 5.49 所示。

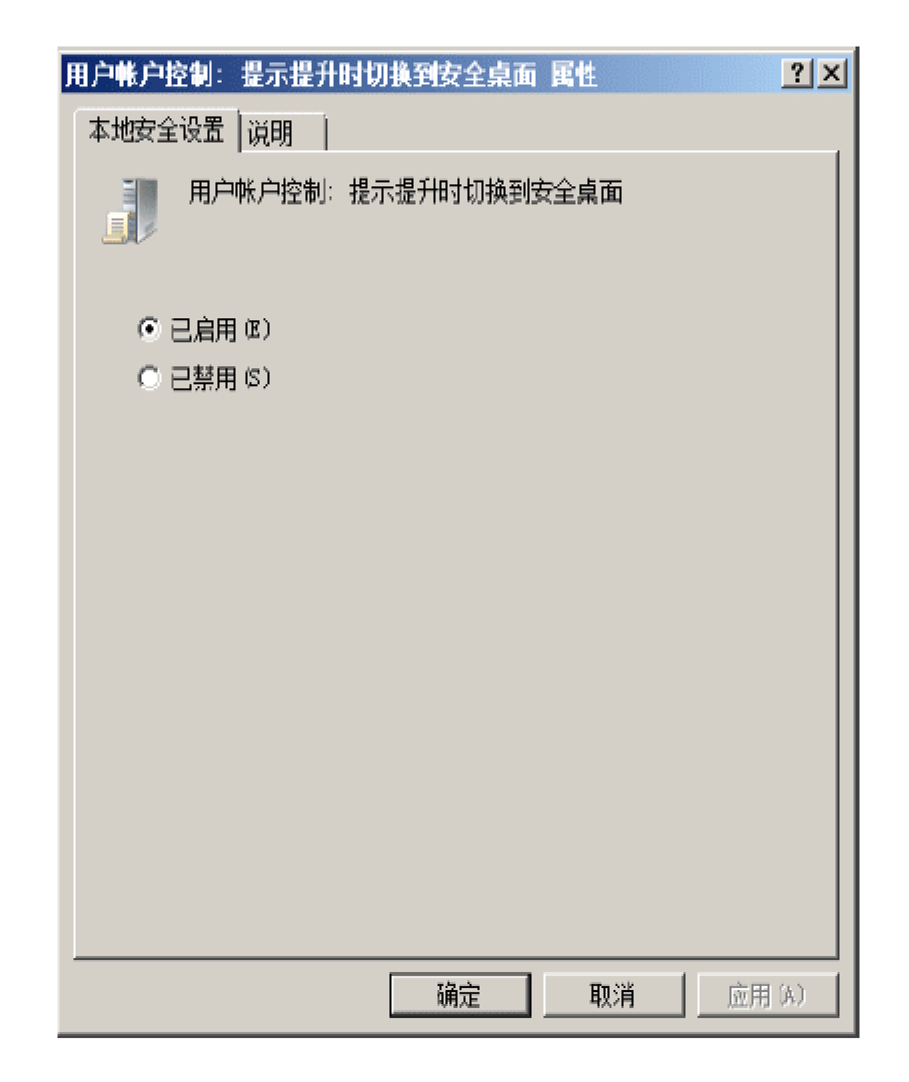


图 5.49 “用户帐户控制：提示提升时切换到安全桌面 属性”对话框

7. 用户帐户控制：以管理员批准模式运行所有管理员

这是 UAC 的开关选项，切不可禁用 UAC，否则所有相关的功能都将关闭，文件和注册表虚拟化也不复存在，用户将会丢失数据。使用管理批准模式的用户，会以完全权限登录，所有程序都将获得管理员权限，并且这一切都不会有任何的提示出现。另外，用于提高 Windows Vista 之前程序兼容性的应用程序兼容性垫片也被禁用了。Internet Explorer 保护模式同样不可用，只能以管理权限运行。默认情况下，此设置是启用的，如图 5.50 所示。

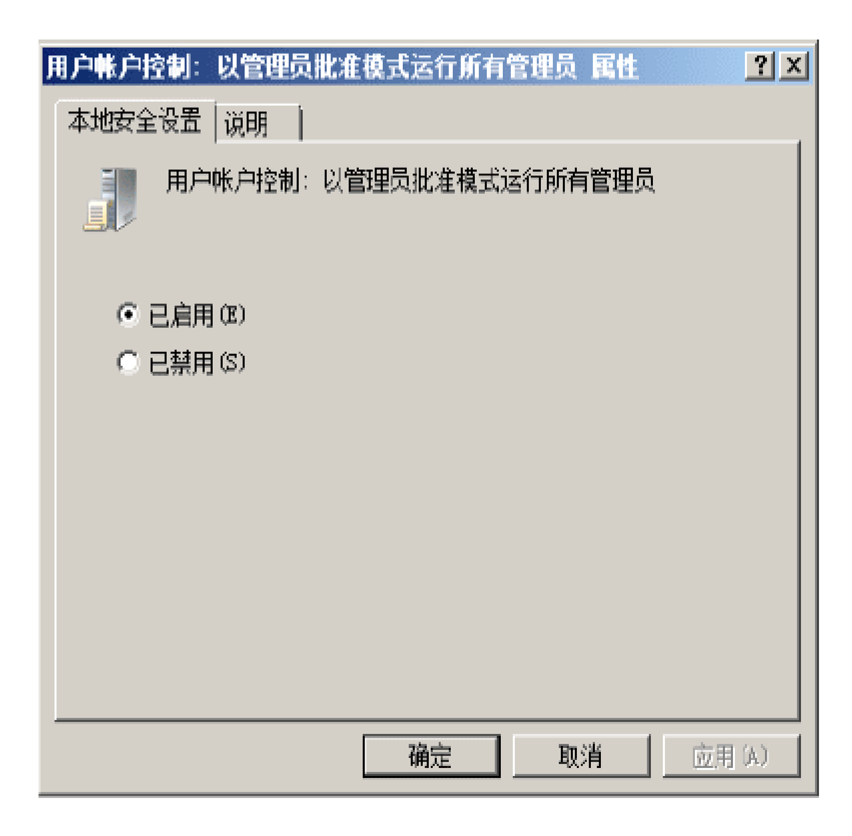


图 5.50 “用户帐户控制：以管理员批准模式运行所有管理员 属性”对话框

8. 用户帐户控制：用于内置 Administrator 帐户的管理员批准模式

此安全设置控制内置 Administrator 帐户的行为。如果将内置管理员帐户用于日常工作，则应当禁用此设置。不过禁用后，就不能使用 IE 保护模式了，所有的程序都会以管理员权限运行。

双击“用户帐户控制：用于内置 Administrator 帐户的管理员批准模式”策略，显示如图 5.51 所示对话框。在“本地安全设置”选项卡中，选择“已启用”单选按钮，启用该策略。单击“确定”按钮保存设置即可。

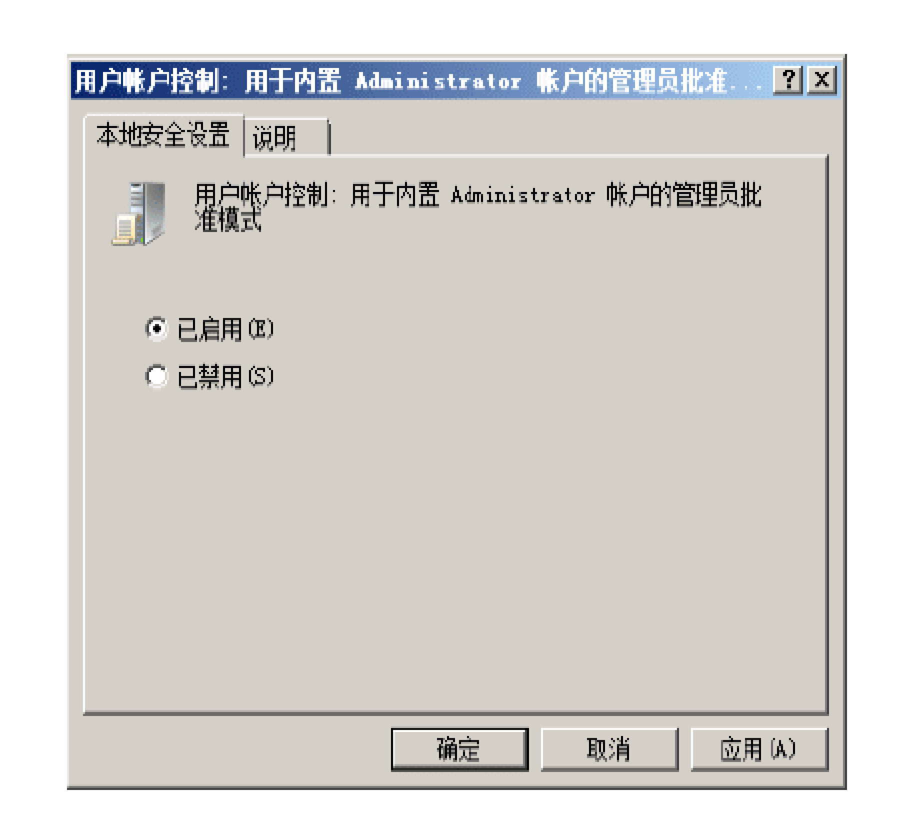


图 5.51　“用户帐户控制：用于内置 Administrator 帐户的管理员批准模式 属性”对话框

9. 用户帐户控制：允许 UIAccess 应用程序在不适用安全桌面的情况下提示提升

此安全设置控制 UIAccess 或 UIA 程序是否可以自动禁止标准用户使用提升提示的安全桌面。如果启用此设置，包含 Windows 远程协助的 UIA 程序可以自动禁用提升提示的安全桌面。除非还禁用了提升提示，否则提示会出现在交互式用户桌面而不是安全桌面上。默认情况下，该设置是禁用的，如图 5.52 所示。

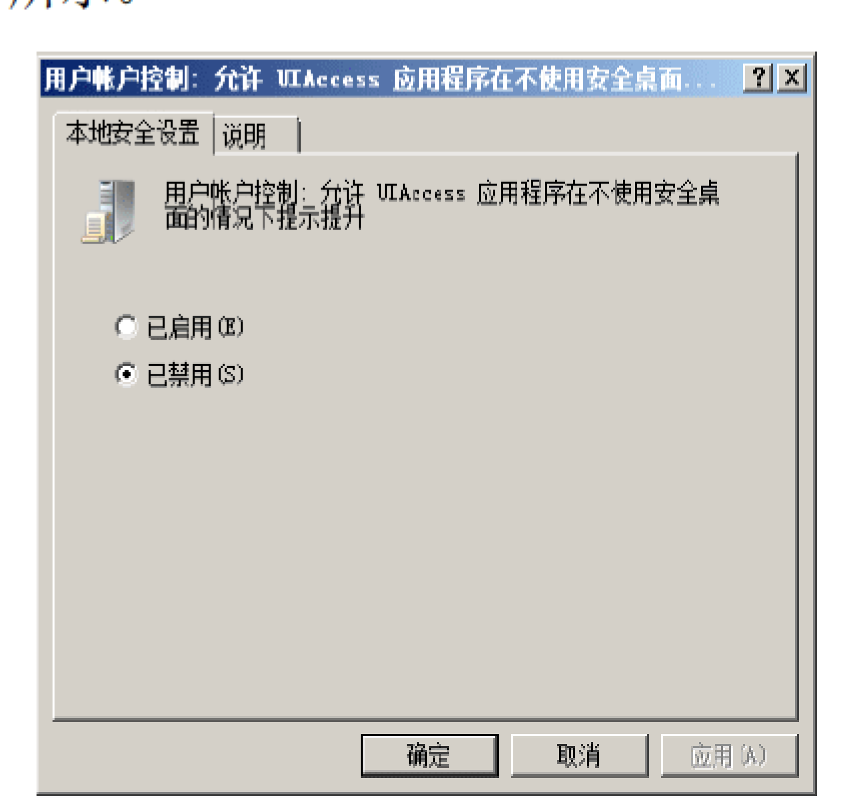


图 5.52　“用户帐户控制：允许 UIAcess 应用程序在不使用安全桌面的情况下提示提升 属性”对话框

此设置禁止 UIAccess 应用程序，比如远程协助，在安全桌面提示提升，而是在 UIAccess 应用程序完成后才启动安全桌面，如图 5.53 所示。对于依赖远程协助来为终端用户桌面提供支持的企业而言，此设置非常方便。其默认为禁用。

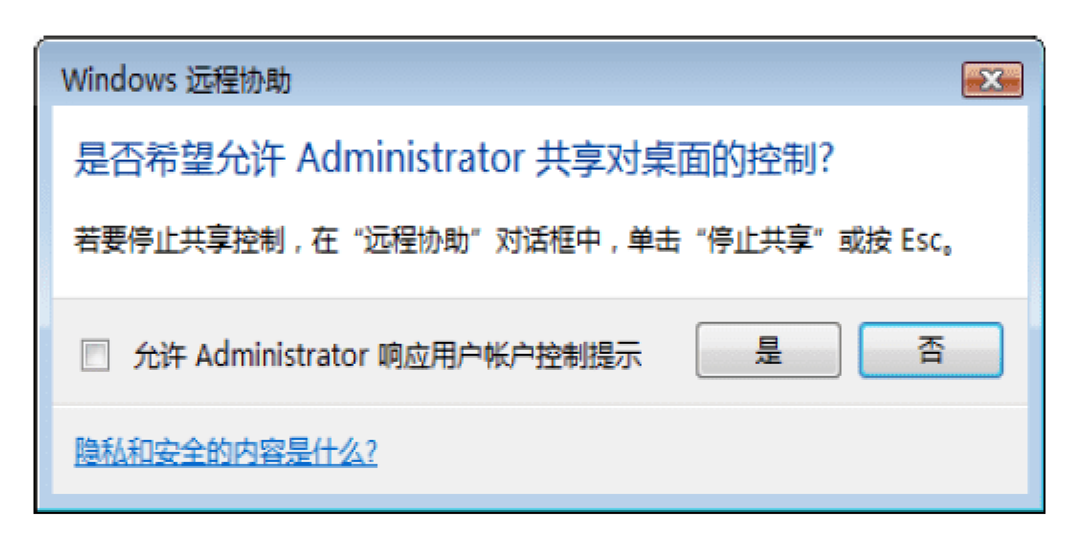


图 5.53　Windows 远程协助

10. 用户帐户控制：只提升签名并验证的可执行文件

此设置将会在交互应用程序请求提升时，核对其代码验证签名。如果企业仅运行代码验证签名的程序，此设置可以提高安全性，因为其能够控制需要提升权限的程序。不过，许多用户在使用此设置时会遇到签名程序兼容性问题，所以此设置默认为禁用的，如图 5.54 所示。

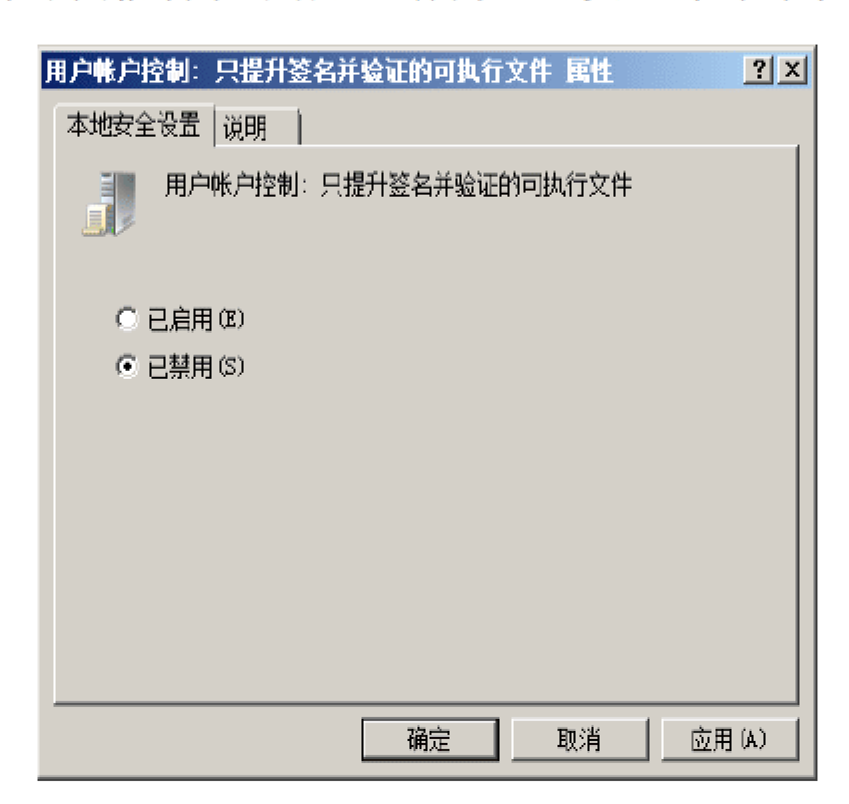


图 5.54 “用户帐户控制：只提升签名并验证的可执行文件 属性”对话框

5.5.4 UAC 相关策略

Windows Vista 和 Windows Server 2008 还有两个补充策略设置：要求输入凭证的受信任路径和在提升设置中列举本地管理员帐户。在“本地组策略编辑器”窗口中，依次展开“本地计算机策略\计算机配置\管理模板\Windows 组件\凭据用户界面”分支，即可查看和编辑 UAC 相关的策略，如图 5.55 所示。

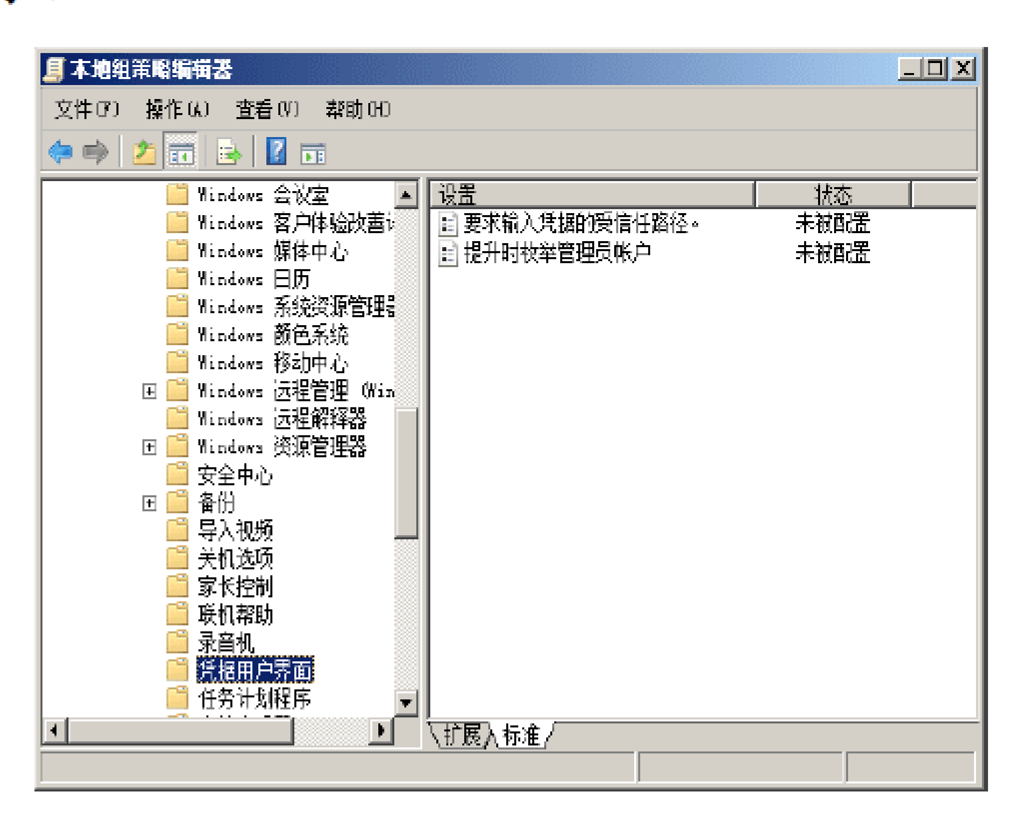


图 5.55 “凭据用户界面”对话框

1. 要求输入凭证的受信任路径

此设置控制用户是否使用受信任路径输入 Windows 凭据。受信任路径指的是一个安全密钥序列，有时指安全警告序列，其能够防止恶意软件盗取 Windows 凭据。当普通用户试图执行需要管理员权限的任务时，系统会强制用户按下“Ctrl+Alt+Delete”组合键，避免其使用伪造的密码获取权限，这就加强了安全性。默认情况下，该策略是未配置的，双击“要求输入凭

据的受信任路径”策略，显示如图 5.56 所示对话框。用户可以根据需要启用或禁用该策略。

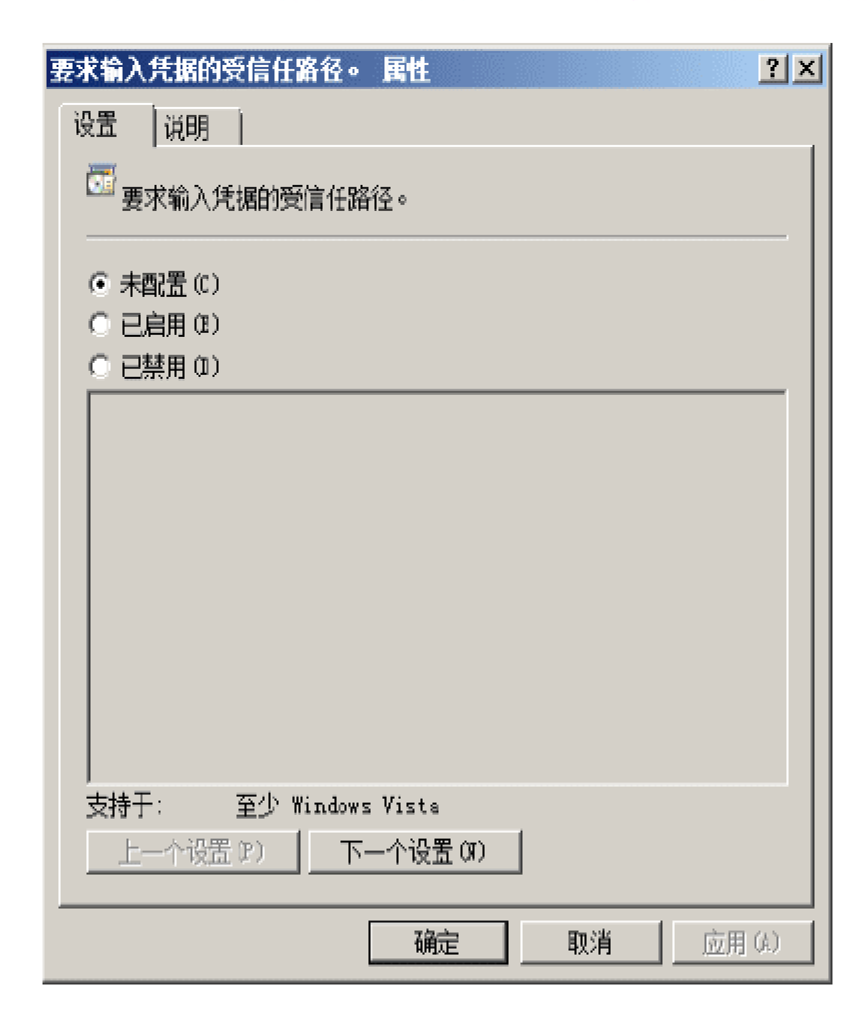


图 5.56　“要求输入凭证的受信任路径。属性”对话框

2. 提升时枚举管理员帐户

默认情况下，该策略是未配置的，即尝试提升正在运行的应用程序时，不会显示管理员帐户。双击“提升时枚举管理员帐户”策略，显示如图 5.57 所示对话框。如果启用此策略设置，则会显示计算机上的所有本地管理员帐户，这样用户便可以从中选择一个帐户并输入正确的密码。如果禁用此策略设置，系统将始终要求用户输入用户名和密码进行提升。

启用此设置后，在 UAC 凭据用户界面中自动列举管理员帐户，如图 5.58 所示。需要注意的是，在某些域环境中，会遇到网络连接问题，如果应用此设置会导致不可预期的延迟。

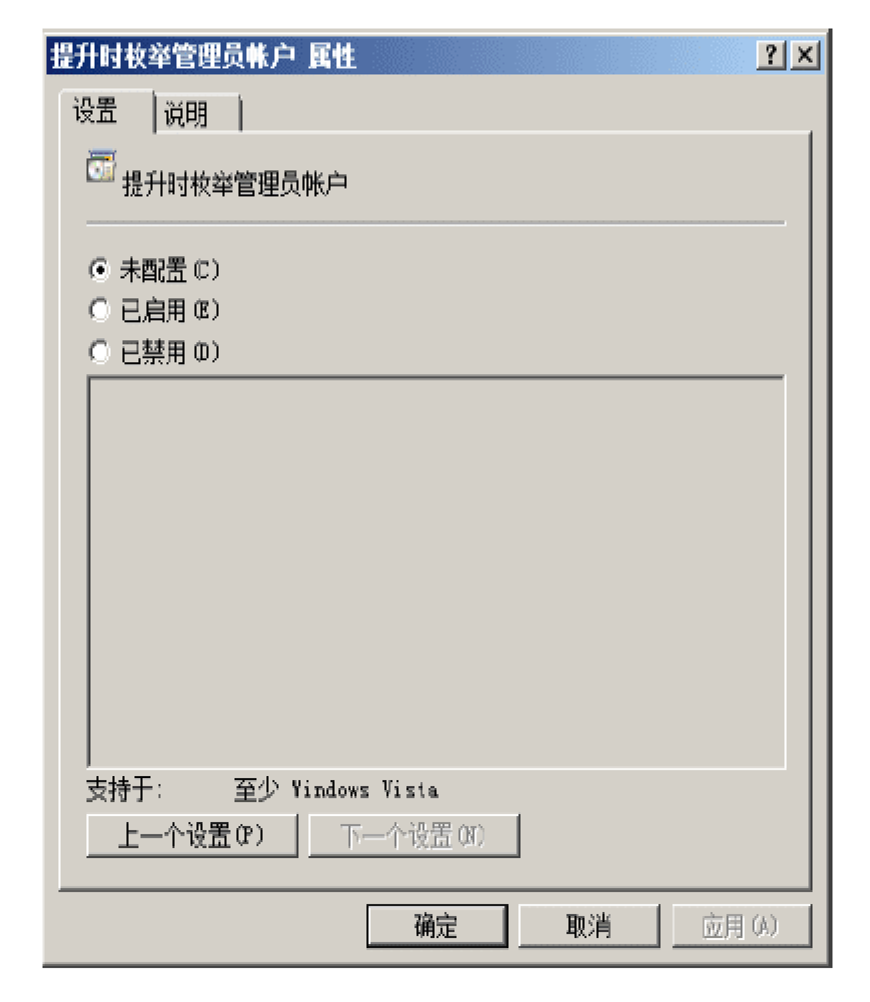


图 5.57　“提升时列举管理员帐户 属性”对话框



图 5.58　自动列举管理员帐户

小　　结

用户是计算机和网络的主体，用户帐户是与用户一一对应的，为了确保系统安全，管理员往往需要针对用户身份的不同，为其对应的帐户分配不同的访问和操作权限。本章主要介绍了Windows Server 2008 系统中，用户帐户的基本安全设置。Administrator 是 Windows Server 2008 默认的系统管理员帐户，也是最易收到攻击的用户帐户之一。通常情况下，用户可以通过设置强密码、定期更改密码、设置陷阱账号等方法，确保管理员帐户的安全。另外，管理员还可以通过设置允许用户帐户登录的计算机和登录时间，限制用户的某些操作。将常用的操作权利分配到不同的用户帐户，即可减轻管理员的工作负担，又可以提高网络安全性。UAC 是 Windows Server 2008 和 Windows Vista 系统中的新增功能，当普通帐户由于受限而未能完成操作时，可以临时向管理员请求相关权限，既可以完成操作，又不会改变其权限设置。

习　　题

1. Windows Server 2008 默认的密码策略是什么？
2. 保证用户帐户安全有哪些方法？（至少列出三个）
3. 如何制作密码重置盘？
4. 限制 zhangsan 的登录时间为星期一到星期五早上 8 点到下午 5 点，星期六到星期天为中午 12 点到下午 6 点的命令是什么？

实验：管理员帐户安全

实验目的

掌握保护系统管理员帐户安全的多种方法。

实验内容

管理员帐户是 Windows 系统中最易受到攻击的用户帐户之一，应从多个方面确保其安全。

实验步骤

1. 重命名管理员帐户。
2. 设置陷阱帐户。
3. 为管理员帐户设置强密码。

第6章

组策略安全

组策略（Group Policy）是一种基于组对象的高效管理机制，可以帮助管理员批量完成网络客户端部署任务，包括安全配置、用户环境设置、软件分发、用户帐户策略等。在 Windows 域环境中，管理员可以通过组策略限制用户可在服务器上进行的操作，以提高服务器的安全性。

本章导读

- 组策略概述
- 组策略模板
- 软件限制策略
- 硬件限制策略

Windows Server 2008

6.1 组策略概述

组策略是管理员为用户和计算机定义并控制程序、网络资源以及操作系统管理的一种主要工具。在 Windows Server 2008 Active Directory 环境中，管理员可以管理整个域中用户桌面环境，例如限制用户使用特定的程序、设置用户的桌面环境、添加登录脚本等。

6.1.1 组策略的功能

组策略不仅应用于用户和客户端计算机，而且还应用于在管理范围内的成员服务器、域控制器。在默认情况下，应用于域的组策略将影响到域中所有的计算机和用户。“Active Directory 用户和计算机”还提供了内置的域控制器。管理员可以通过 GPO（组策略对象）默认域控器制策略，将域控制器与其他计算机分开进行管理。

6.1.2 组策略的组件

组策略组件包括组策略对象组件、组策略容器组件、客户端扩展组件、组策略模板组件、组策略编辑器组件、计算机策略和用户策略组件、组策略和本地策略组件。

1. 组策略对象组件

在活动目录中，站点、域和组织单位内的容器对象都可以连接到一个 GPO 中。通过连接，可以将 GPO 设置应用于指定容器中的用户和计算机。GPO 由组策略容器（GPC）和组策略模板（GPT）两个部分组成。

2. 组策略容器组件

组策略容器组件（Group Policy Container，简称 GPC）是一个活动目录对象，它列出了一个特定 GPO 管理的 GPT 名称。当 Windows 客户端下载和处理 GPT 信息时，需要使用 GPC 信息来确定。

3. 客户端扩展组件

客户端扩展组件（Client Side Extension，简称 CSE）在 Windows 客户端上有许多功能是由组策略来管理的，这些功能都具备相应的服务，不仅可以知道如何获取和处理组策略，而且称这些服务为“客户端扩展组件”，是以动态链接库形式存在。

4. 组策略模板组件

组策略模板组件（Group Policy Template，简称 GPT），实现了一系列的指令集。例如，对

注册表进行更新的组策略存储在名为 Registry.pol 的 GPT 文件中，如图 6.1 所示。

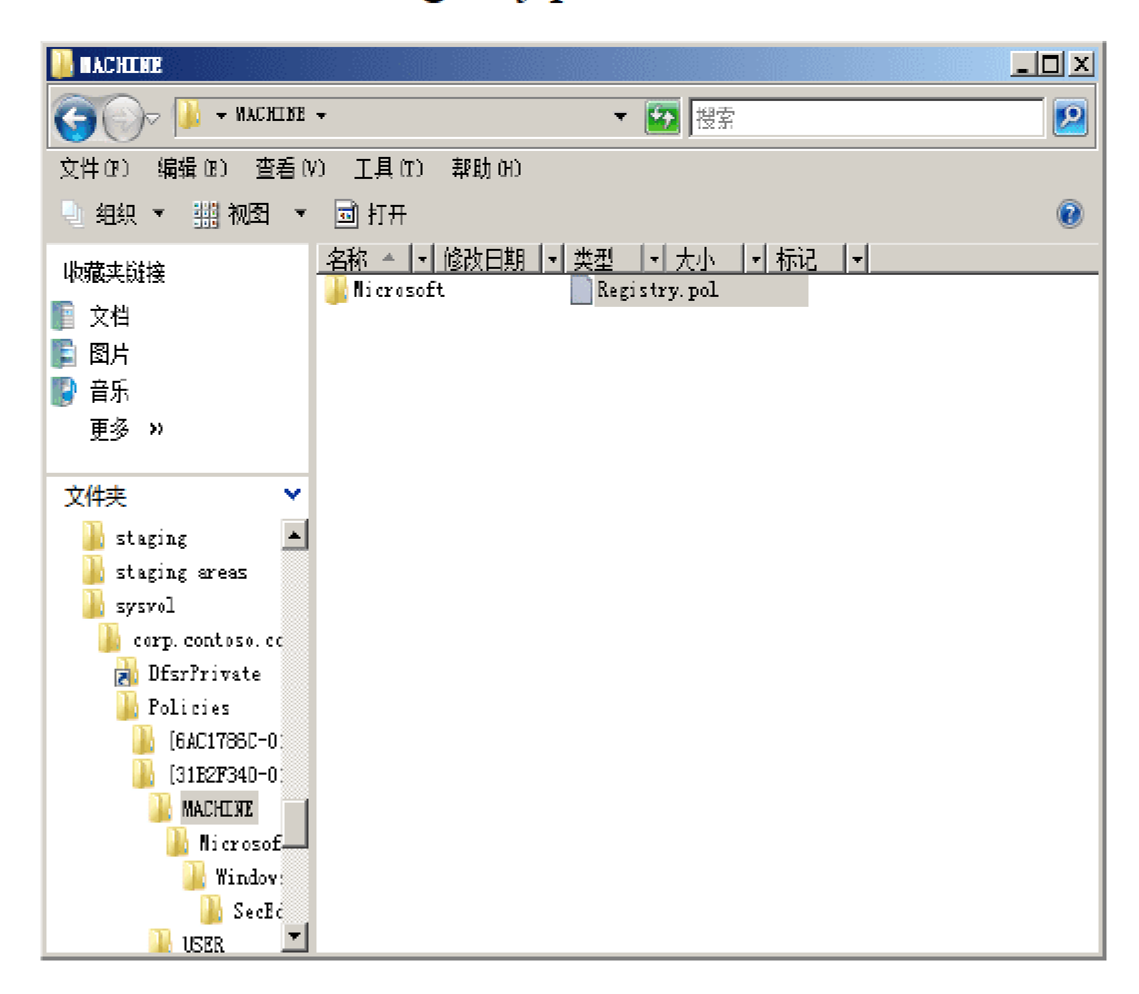


图 6.1　标准 GPT 文件在 Sysvol 的位置

5. 组策略编辑器组件

组策略编辑器组件（Group Policy Editor，简称 GPE），是一个 MMC 管理单元，用户创建和管理 GP0。

6. 计算机策略和用户策略组件

组策略对象设置可以应用于计算机对象和用户对象。

7. 组策略和本地策略组件

每个客户端都有自己的本地策略，如果用户是域成员则登录时下载域策略，如果不是域成员，那么登录时使用本地策略。

6.2　组策略模板

管理模板是基于注册表的策略设置，通过管理模板的定制，可以在统一界面下实现对相关组策略的编辑和设置，从而有效地实现组策略的管理效率。在 Windows 2000/XP/2003 系统中，策略模板文件一直使用单独文件格式，即.adm 文件。传统的.adm 模板文件虽然为修改注册表提供了必要的方法，但也并非尽善尽美。在 Windows Server 2008 系统中，采用了全新文件格式的策略模板，即.admx，新策略模板文件的出现，使 Windows Vista 或 Windows Server 2008 用户管理基于注册表的策略设置变得更加简便。

6.2.1 Windows Server 2008 中组策略的新特性

在 Windows Server 2008 系统中对原有的系统策略进行了扩展，Windows server 2003 SP1 中提供了约 1700 条组策略设置，但是在 Windows Server 2008 系统中已增加至 2400 条组策略，管理功能更加丰富。在 Windows Server 2008 系统中，组策略管理控制台提供了更多元化的组策略管理方式，主要有以下新特点：

- 支持新的策略应用范围，包括无线和有线网络、Windows 防火墙和 IPsec 策略，支持电源管理和 USB 设备限制策略；
- 客户和域控制器之间慢速链接检测已经有所改进，现在可以有一个更稳定的机制，来判定客户是否通过慢速链接连接到域控制器，从而决定所应用的组策略行为；
- 组策略更新现在是基于域控制器的可用性，也就是说，当客户远程通过 VPN 链接到网络的时候，组策略更新会更加及时；
- 支持多个本地策略对象（LGPO）以及针对不同的用户组或用户设置不同的组策略对象；
- 支持基于 XML 的管理模板文件格式化（ADMX），更好地支持多语言模板；
- 支持 per-GPO 和 per-GP 的设置；
- GPMC 和组策略编辑器都有了改进，并且增加了新功能；
- 增加了通过收购 Desktop Standard 所获得的工具，也就是现在被称为 Group Policy Preferences 的工具，用它来实现组策略的自动创建。

6.2.2 ADMX 和 ADM 文件

新的 ADMX 文件格式和自 Windows NT 4.0 起便存在的旧 ADM 格式最大的区别在于，ADMX 采用了 XML 标准来描述注册表策略的设置。首先，编辑 XML 的工具要远多于编辑 ADM 语法的工具。其次，由于 XML 是架构化的，因此最终会比较容易构建一些工具，来帮助用户在正确位置放置正确的标记，进而创建结构良好的 ADMX 文件。其中架构化是指对于给定的 XML 应用程序（如 ADMX 格式），有一个文档化的架构来描述可能用到的元素和属性以及它们的组织方式。本文后面的部分将对一个示例进行分析。

1. ADMX 和 ADM 文件的区别

ADMX 和 ADM 的另一个主要区别在于主 ADMX 文件的字符串部分分到了语言特定的 ADML（ADM Language，ADM 语言）文件中。如果熟悉 ADM 文件，就会知道每个文件的结尾会有一个以“[strings]”标记分隔的部分，其中用户可以为字符串赋值，该字符串会在使用组策略编辑器和管理模板时显示。例如，单击给定策略的“解释”选项卡时所看到的文本，就存储在该字符串部分中。问题是字符串存储在 ADM 文件中，如果希望在其他语言的 Windows 系统上使用该 ADM，则需要创建一个新的 ADM 文件，并加上适用于该语言的字符串部分。

ADM 文件本身默认被保存在组策略的 SYSVOL 目录下的“组策略模板”中，因此每当创

建一个 GPO，就会在每个域控制器上占用大约 4 MB 的存储空间，并且组策略模板对于在其他工作站上编辑组策略都是必不可少的，没有相应的 ADM 文件，就无法编辑包含在 GPO 内的任何自定义设置。使用 ADMX 格式，就避免了这些问题。用户不必再将任何内容直接存储在 GPO 内部，因此不会出现通常所说的“SYSVOL 膨胀”。新 ADMX 标准可以利用“中心库”所具备的优势，存储新的 ADMX 文件，而不必将它们复制到每个 GPO 中。“中心库”的另一重要作用是：如果 ADMX 文件具有更新的定义，则所有管理工作站将立即使用更新的 ADMX 文件。

新的 ADMX 和 ADML 文件同样具有新的存储模型，在 Windows Server 2008 系统中默认存储的路径是%windir%\policydefinitions，如图 6.2 所示。

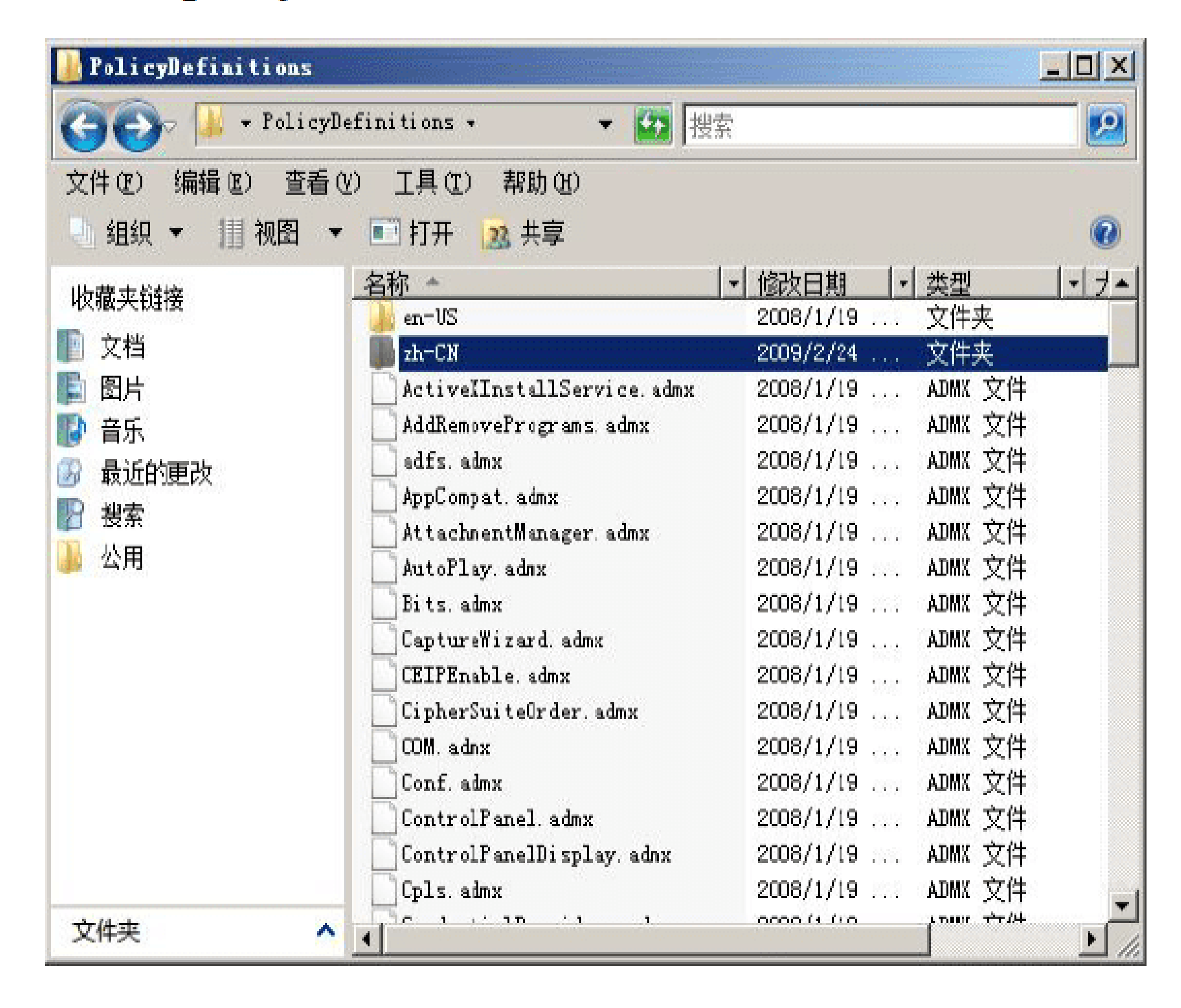


图 6.2　查看 Windows Server 2008 中的 ADMX 文件

ADMX 文件存储目录下的 en-US 和 zh-CN 文件夹，分别用于存储中文和美式英语的 ADML 文件。当启动组策略编辑器，展开管理模板节点的时候，编辑器会自动查找到%windir%\policydefinitions 文件夹。当然也可以把这些文件复制到中央位置，例如中央存储。

中央存储是在 Sysvol 中创建的域范围的目录，降低因 GPO 数量的不断增加而导致的其他存储和更大复制通信的需求。创建中央存储之前，组策略管理工具使用本地计算机中的核心操作系统 ADMX 文件。此外，管理工具还可以读取在本地存储或在 GPO 中存储的任何其他 ADM 文件。这将确保不同平台管理之间的互操作性。仅存在于 ADMX 文件中的所有策略设置只能在平台上使用。

ADMX 和 ADML 文件不会自动复制到 GPO 的 Sysvol 中。如果创建一个新的 GPO，则默认不包含任何 ADMX 文件。所有的 ADMX 和 ADML 文件，都是编辑 GPO 的时候添加进去的。这样可以节省域控制器中 Sysvol 的存储空间，因为临时文件不再存储于每个域控制器上了。

2. ADMX 的中央存储

Windows Vista 和 Windows Server 2008 中的一个显著特性，就是 ADMX 中央存储。在之前版本的 Windows 系统中，ADM 模板的主要功能就是生成组策略的管理模板，并且自动复制到每个 GPO 模板，这种复制机制必然产生一些问题，导致 GPO 的管理和版本控制出错。在 Windows Server 2008 和 Windows Vista 系统中，管理模板文件被基于 XML 的文件格式取代，

并且增加了多语言支持和强版本控制，可以在多语言环境中管理组策略。

为了解决 ADM 模板的复制和管理问题，ADMX 文件被集中在中央存储。管理员只需要在每个域控制器的 C:\Windows\Sysvol\sysvol\<domain name>\Policies 下，创建一个名为 PolicyDefinitions 的文件夹，并将所有的 ADMX 文件复制到该文件夹中即可。

6.2.3 编辑 ADMX 模板

相对于以前操作系统版本所使用的 ADM 文件，Windows Vista/2008 中的 ADMX 格式有了明显的改进。XML 的使用，为编辑和搜索这些文件提供了更为清洁的框架。语言特定字符串向单独文件的转换，使得多语言组策略编辑能够无缝进行。同时，中心库消除了将所有 GPO 与 ADM 文件的副本一同存储并更新的必要性。用 XML 编写 ADMX 的确是一大进步，但是，许多管理员并不知道如何编写 XML，更不用说了解 ADMX 用于创建策略扩展的架构了。管理员可以使用多种编辑工具打开或编辑 ADMX 或 ADML 文件，如记事本、文本编辑器、Visual Studio 等，甚至在 IE 浏览器中可以查看文件详细内容。如图 6.3 所示在记事本中打开的系统默认的 XML 文件。

```
IndependentRolesLoc.xml - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
<?xml version="1.0" encoding="utf-16"?>
<!--Version 2.2-->
<SCWLocalization CultureName="en-US">
    <RoleLocalization>
        <Role Name="Core">
            <DisplayName>Core</DisplayName>
            <Description>Services required for all roles.</Description>
        </Role>
        <Role Name="SecurityandNetwork">
            <DisplayName>Security and Network</DisplayName>
            <Description>Enables network infrastructure and security services.</Description>
        </Role>
        <Role Name="Independent">
            <DisplayName>Independent</DisplayName>
            <Description>The independent role consists of Windows services that cannot be en
        </Role>
    </RoleLocalization>
    <ServiceLocalization>
        <Service Name="Appinfo">
        </Service>
        <Service Name="DcomLaunch">
        </Service>
        <Service Name="Dhcp">
        </Service>
        <Service Name="Eventlog">
        </Service>
        <Service Name="EventSystem">
        </Service>
        <Service Name="PlugPlay">
```

图 6.3 使用记事本编辑 XML 文件

6.3 安全策略

安全策略是影响计算机上安全设置的集合，通过“安全设置”工具可以更改组策略对象的安全配置。通过安全策略设置可以影响多台计算机，有利于保护计算机和网络上的资源。

6.3.1　帐户策略

帐户策略可以设定用户在被系统拒绝之前以及密码帐户过期时，允许进行多次登录尝试。通过设定密码过期日期，可以强迫用户定期更改密码，限制允许用户登录的时间等。通过建立严格的帐户管理策略，有效地挫败肆意和无意识的密码攻击。

1. 密码策略

在密码策略中包含以下 6 个策略。

（1）密码必须符合复杂性要求

此安全设置确定密码是否符合复杂性要求。如果启用此策略，则密码必须符合 Windows Server 2008 用户帐户密码策略，详细内容请参考本书“第 5 章 用户帐户安全”中的相关介绍。

01 打开“组策略管理编辑器”窗口，依次选择“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“帐户策略”→“密码策略”选项，在右侧窗格中双击“密码必须符合复杂性要求”选项，显示如图 6.4 所示“密码必须符合复杂性要求 属性”对话框。

02 选中“定义这个策略设置”复选框，选择“已启用”单选按钮，单击“确定”按钮即可。



提示　在域控制器上，默认已经启用，独立服务器上则为禁用。

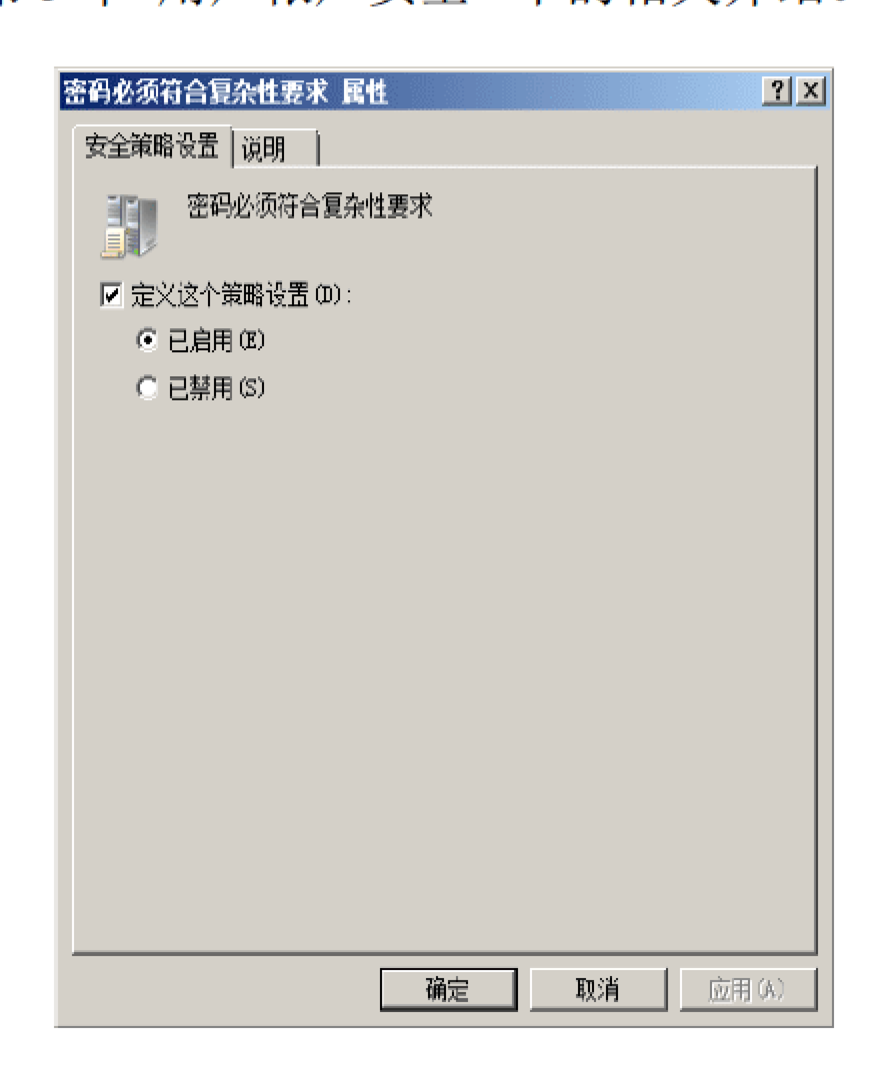


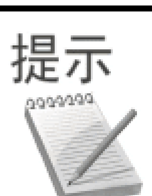
图 6.4　“密码必须符合复杂性要求 属性”对话框

（2）密码长度最小值

此安全设置用于确定用户帐户密码包含的最少字符数，可以设置 0 到 14 中的任何一个值。

01 在“组策略管理编辑器”窗口中，依次选择“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“帐户策略”→“密码策略”选项，在右侧窗格中双击“密码长度最小值”选项，显示如图 6.5 所示“密码长度最小值 属性”对话框。

02 选中“定义这个设置”复选框，在“密码必须至少是”文本框中输入密码长度，单击“确定”按钮即可。



提示　默认情况下，在域控制器上的值为 7，在独立服务器上的值为 0。

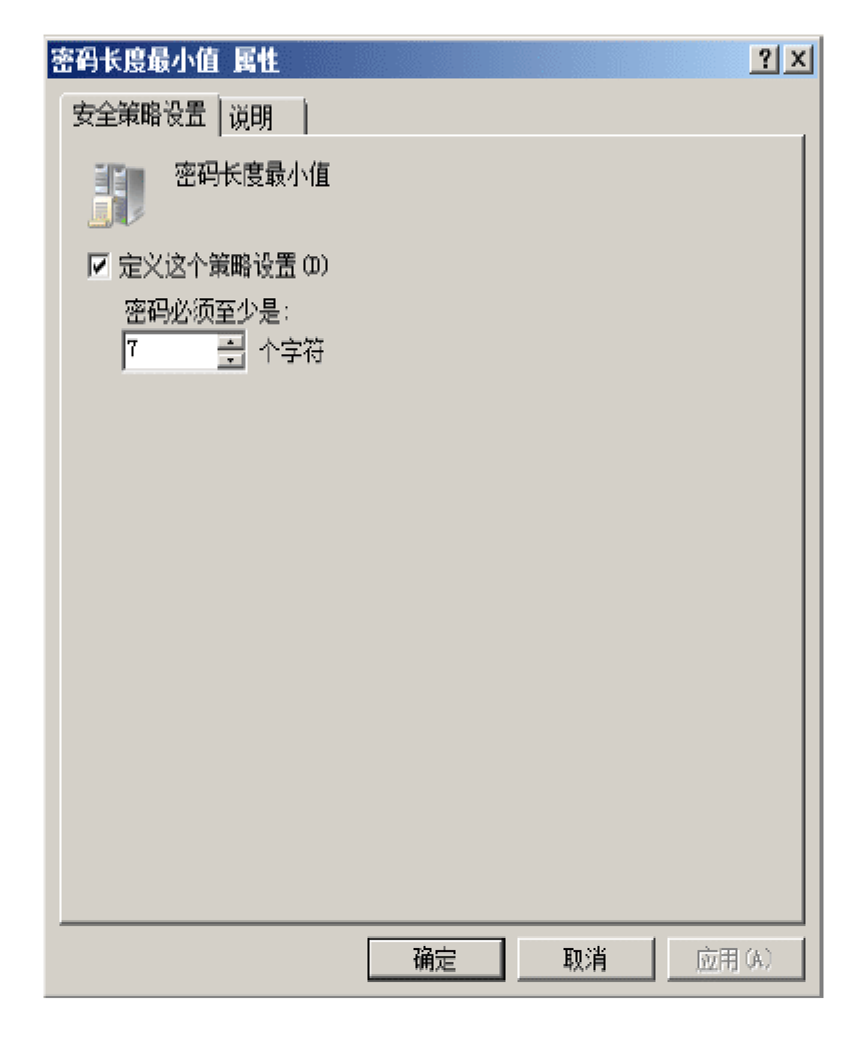


图 6.5　“密码长度最小值 属性”对话框

（3）密码最短使用期限

该安全设置要求用户在更改密码之前必须使用该密码一段时间（以“天”为单位）。设置范围为 1 到 999 之间的值。如果将天数设置为 0，则表示允许用户立即更改密码。

01 在“组策略管理编辑器”窗口中，依次选择“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“帐户策略”→“密码策略”选项，在右侧窗格中双击“密码最短使用期限”选项，显示如图 6.6 所示“密码最短使用期限 属性”对话框。

02 选中“定义这个策略设置”复选框，在“在以下天数后可以更改密码”文本框中，输入可以更改的天数，单击“确定”按钮即可。

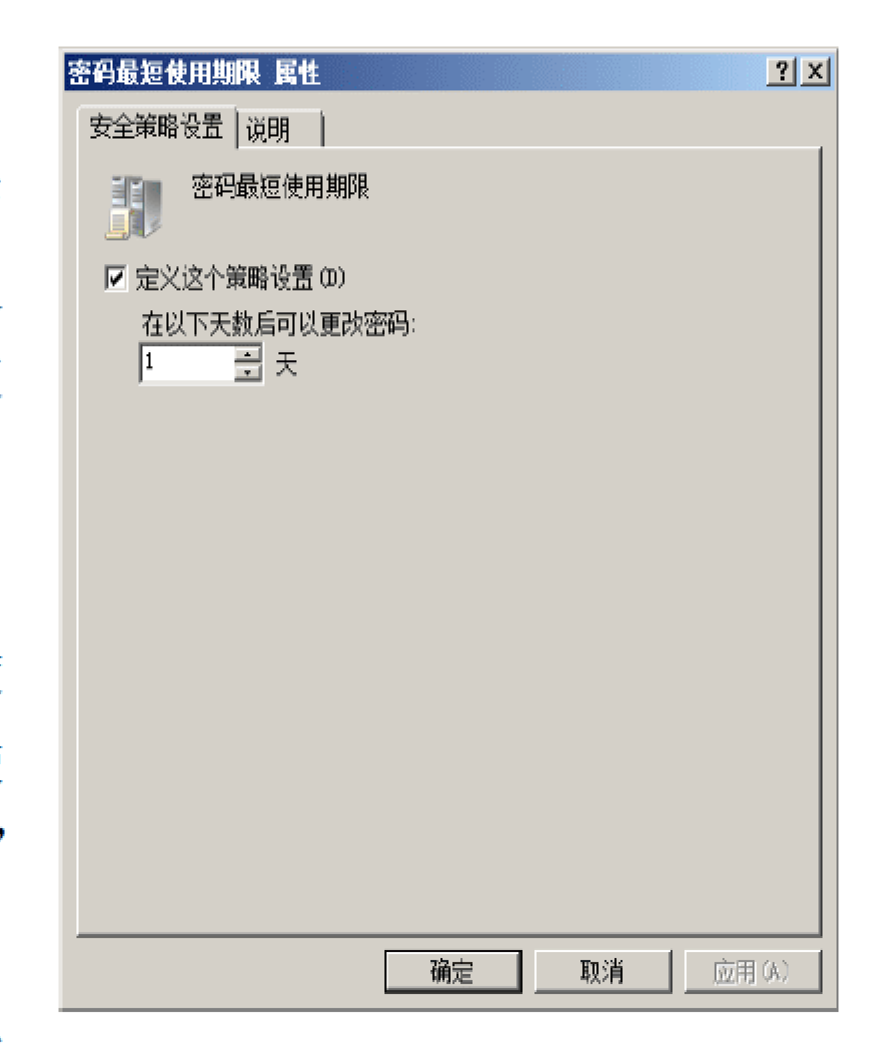


图 6.6 “密码最短使用期限”对话框

注意 密码最短使用期限必须小于密码最长使用期限。在域控制器上默认值为 1，在独立服务器上默认设置为 0。

（4）密码最长使用期限

该设置用户更改某个密码使用之前可以使用该密码的期间（以天为单位）。设置范围介于 1 到 999 之间，如果将密码设置为 0，指密码永不过期。

01 在“组策略管理编辑器”窗口中，依次选择“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“帐户策略”→“密码策略”选项，在右侧窗格中双击“密码最长使用期限”选项，显示如图 6.7 所示“密码最长使用期限 属性”对话框。

02 选中“定义这个策略设置”复选框，在“密码过期时间”文本框中输入密码过期天数。



提示 一般情况下安全最佳操作是将 30 到 90 天后过期，这样入侵者用来破解用户密码以及访问网络资源的时间将受到限制。

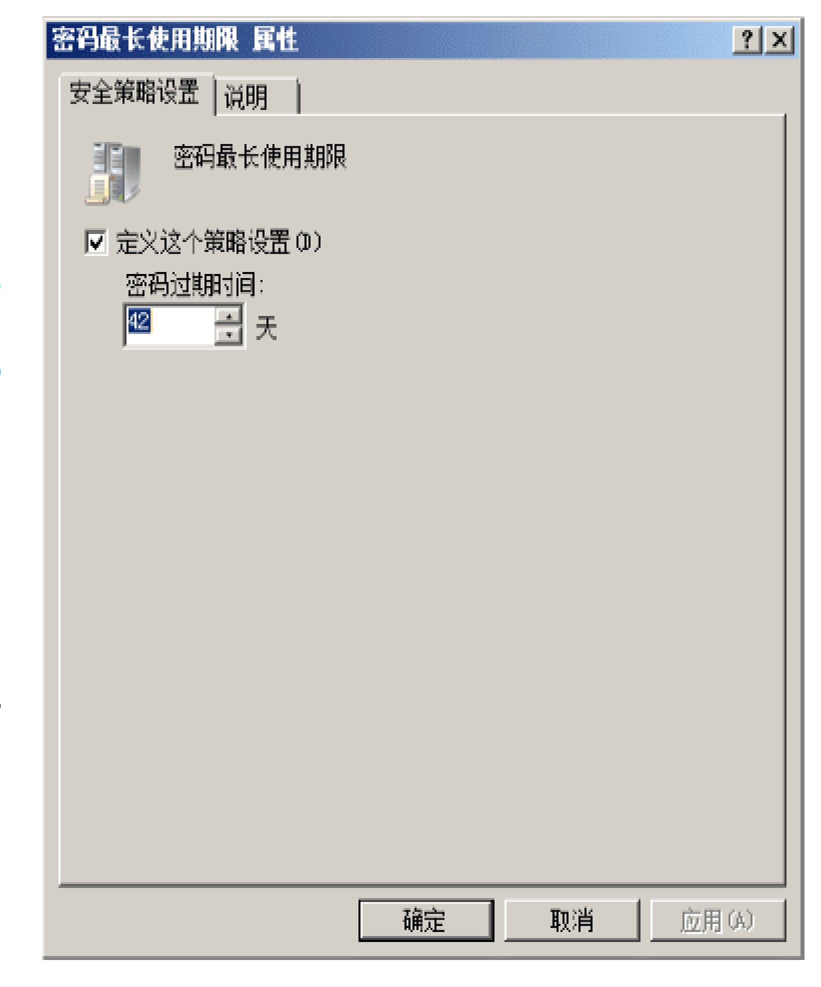


图 6.7 “密码最长使用期限 属性”对话框

（5）强制密码历史

该策略确保旧密码不被连续重新使用来增强安全性。

01 在“组策略管理编辑器”窗口中，依次选择“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“帐户策略”→“密码策略”选项，在右侧窗格中双击“强制密码历史”选项，显示如图 6.8 所示“强制密码历史 属性”对话框。

02 选中“定义这个策略设置”复选框，在“保留密码历史”文本框中输入许可的密码数，单击“确定”按钮即可。

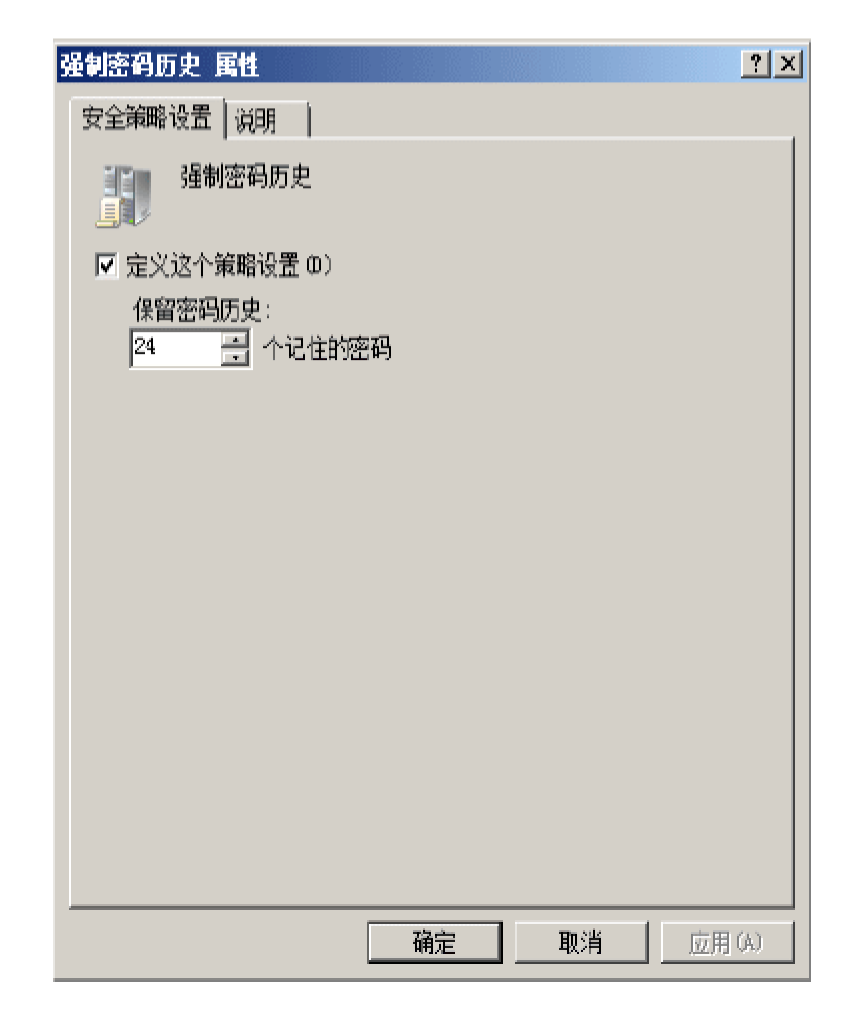


图 6.8　“强制密码历史 属性”对话框

> 提示　在域控制器上的默认值为 24，在独立服务器上的默认值为 0。

（6）用可还原的加密来存储密码

该安全设置确定操作系统是否使用可还原的加密来存储密码。如果某些应用程序使用的协议需要用户密码来进行省份验证，侧策略没这些应用程序提供支持。

01 在“组策略管理编辑器”窗口中，依次选择“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“帐户策略”→“密码策略”选项，在右侧窗格中双击“用可还原的加密来存储密码”选项，显示如图 6.9 所示“用可还原的加密来存储密码 属性”对话框。

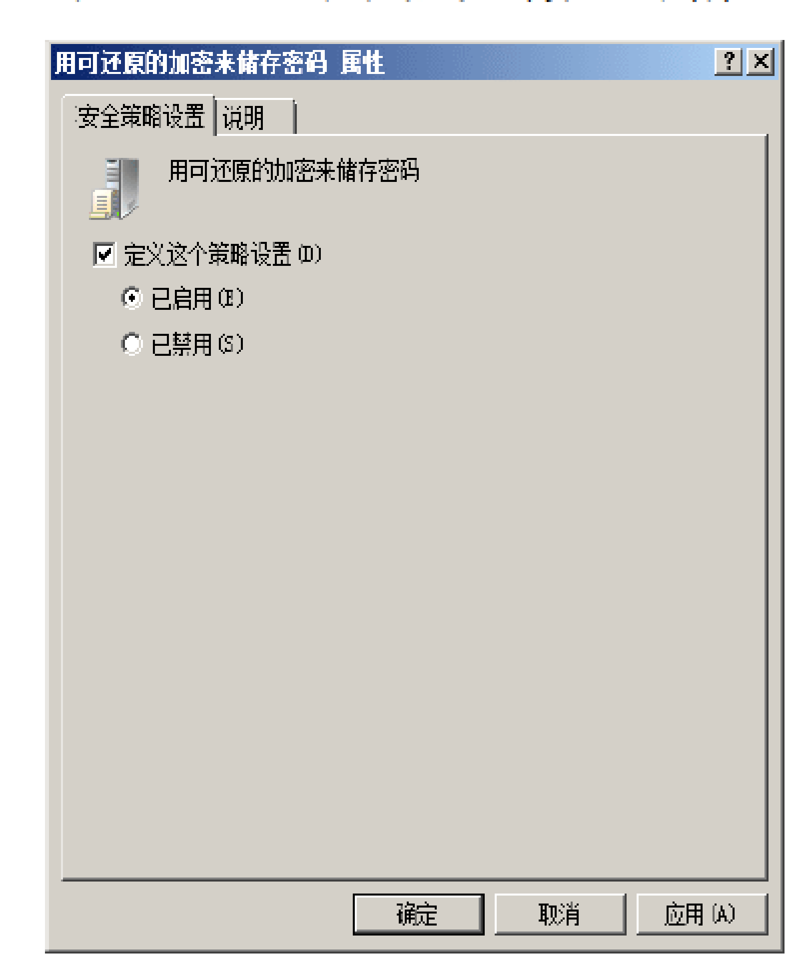


图 6.9　“用可还原的加密来存储密码属性”对话框

02 选中“定义这个策略设置”复选框，选中“已启用”单选按钮，单击“确定”按钮即可。



> 提示　使用可还原的加密存储密码与存储纯文本密码本质上是相同的，除非应用程序比保护密码信息更重要，否则不应启用此策略。系统默认设置为禁用。

2. 帐户锁定策略

帐户锁定策略应用于域用户帐户和本地用户帐户，用来确定帐户的锁定的时间和阈值。

（1）复位帐户锁定计数器

该安全设置确定在登录尝试失败计数器被复位为 0 之前，尝试登录失败之后所需的时间。有效范围为 1 到 99 999 分钟。

01 打开“组策略管理编辑器”窗口，选择“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“帐户策略”→“帐户锁定策略”选项，在右侧窗格中双击“复位帐户锁定计数器”选项，显示如图 6.10 所示“复位帐户锁定计数器 属性”对话框。

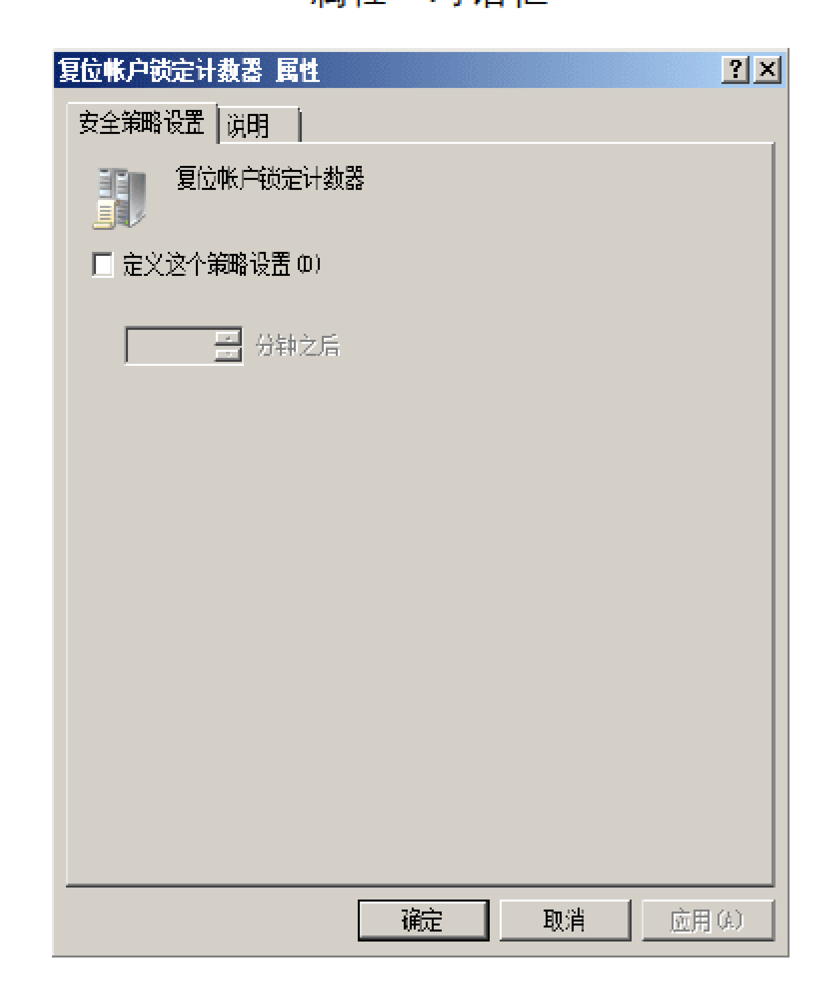


图 6.10　“复位帐户锁定计数器属性”对话框

02 选中“定义这个策略设置”复选框，然后在文本框中输入帐户复位锁定时间，单击“确定”按钮即可。

注意　只有在指定了帐户锁定阈值时，复位帐户锁定计数器才有意义。

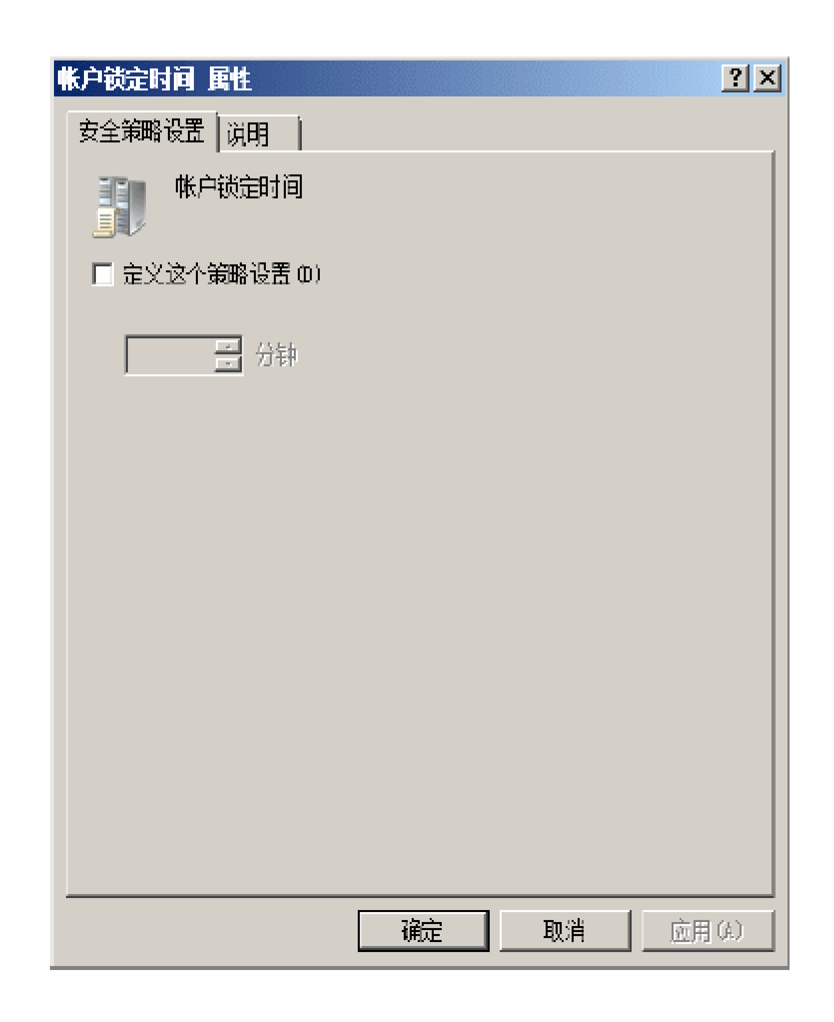


图 6.11　“帐户锁定时间 属性”对话框

（2）帐户锁定时间

该设置确定帐户在自动解锁之前保持锁定的时间。时间范围为 0 到 99 999 分钟，如果帐户锁定时间为 0，则该帐户将一直被锁定直到管理员明确解除对它的锁定。

01 打开“组策略管理编辑器”窗口，选择“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“帐户策略”→“帐户锁定策略”选项，在右侧窗格中双击“帐户锁定时间”选项，显示如图 6.11 所示“帐户锁定时间 属性”对话框。

02 选中“定义这个策略设置”复选框，在文本框中输入锁定时间长度，单击“确定”按钮即可。

提示

只有设置了帐户锁定阈值是，此策略设置才有意义。

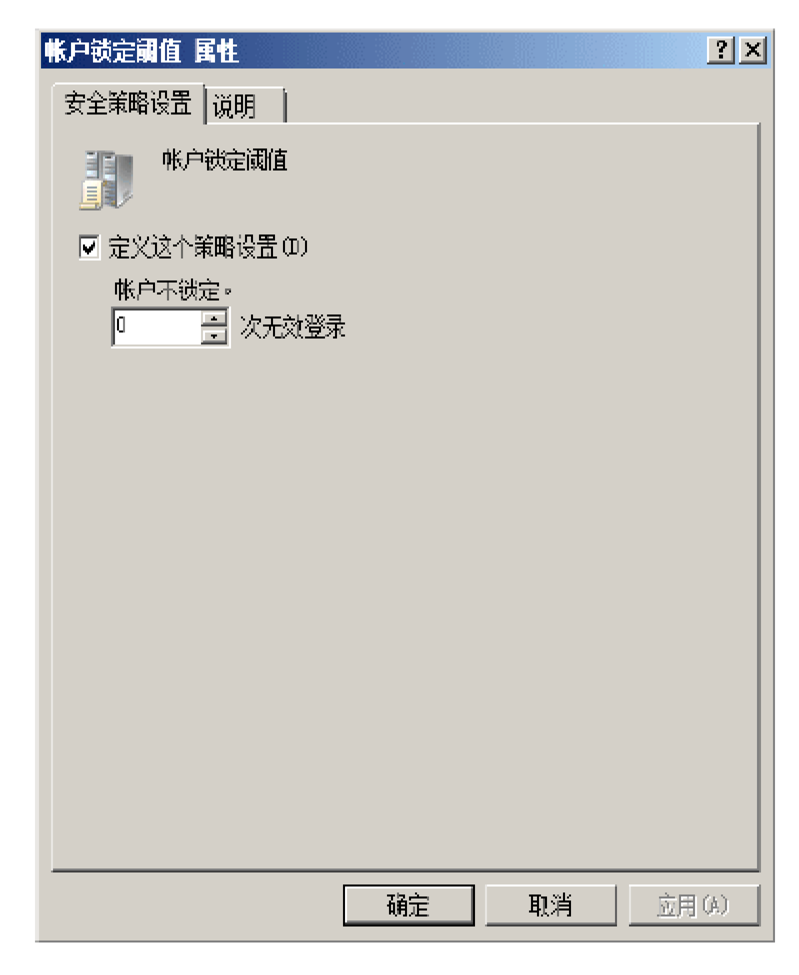


图 6.12　“帐户锁定阈值 属性”对话框

（3）帐户锁定阈值

该设置可以导致用户帐户被锁定尝试登录失败的次数，在管理员解锁该帐户，否则无法使用该锁定帐户，从而降低了用户密码被破解的可能性。

01 在“组策略管理编辑器”窗口中，依次选择“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“帐户策略”→“帐户锁定策略”选项，在右侧窗格中双击“帐户锁定阈值”选项，显示如图 6.12 所示“帐户锁定阈值 属性”对话框。

02 选中“定义这个策略设置”复选框，然后在“帐户不锁定”文本框中输入无效登录的次数。

3. Kerberos 策略设置

Kerberos 策略是活动目录使用的默认认证方式，自动活动目录使用 Kerberos 作为必要的认证方式后，该策略对域 GPO 具有重要作用。如表 6.1 所示列出了 Kerberos 选项的推荐设置。

表 6.1　Kerberos 选项的一些推荐设置

Kerberos 选项	推荐设置
服务票证最长寿命 决定一个 Kerberos 服务票证的可用时间（以分钟为单位）。该选项的值必须介于 10 分钟和“用户票证最长寿命”设置值之间。默认的域 GPO 中这个选项被设置为 600 分钟 注意　当创建一个到服务器的新连接时，过期的服务票证只会被更新，如果一个已建立的会话的票证过期了，会话并不会中断	600 分钟

（续表）

Kerberos 选项	推荐设置
计算机时钟同步的最大容差 设定了 KDC 和客户端计算机时钟时间差距的最大值（以分钟为单位），为了防止轮番攻击，Kerberos 使用了时间戳。因此为了时间戳能正常工作，KDC 和客户端时钟尽可能保持同步是很重要的。在默认的域 GPO 中，这个选项被设置为 5 分钟	5 分钟
用户票证续订最长寿命 设置可以续订 TGT 的最大期限（以天为单位）。默认的域 GPO 中这个选项被设置为 7 天	7 天
用户票证最长寿命 决定 Kerberos TGT（ticket-granting ticket，票证授予票证）的最长使用时间（以小时为单位），TGT 到期后，必须重新申请一个新的票证或者更新已有的。默认的域 GPO 中这个选项被设置为 10 小时	10 小时

6.3.2　审核策略

安全审核对于任何企业系统来说都极其重要，可以通过审核日志来发现是否违反安全事件，例如当发现有入侵时，正确的审核设置所生成的审核日志将包含有关此次入侵的重要信息。Windows Server 2008 中审核策略为没有定义即关闭状态，必须手动开启，审核策略设置完成后需要重新启动计算机才能生效。

1. 审核策略更改

该安全设置确定是否审核用户权限分配策略、审核策略或信任策略的每一个更改事件。如果定义该策略设置，可以指定是否审核成功、审核失败或者根本不审核该事件类型。成功审核在成功更改用户权限分配策略、审核策略或信任策略时生成审核项。失败审核在更改用户权限分配策略、审核策略或信任策略失败时生成审核项。

01 在“组策略管理编辑器”窗口中，依次选择“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“本地策略”→“审核策略”选项，显示如图 6.13 所示“审核策略”窗口。

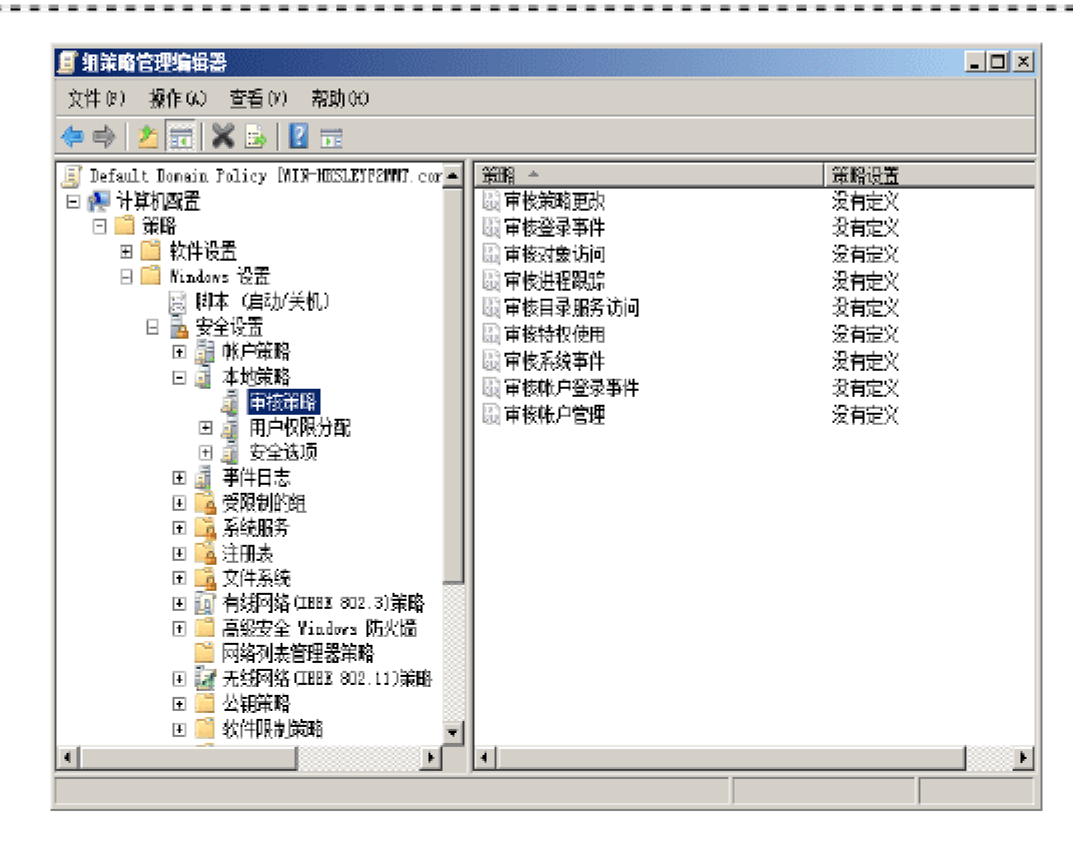


图 6.13　“审核策略”窗口

02 在右侧窗格中双击“审核策略更改”选项，显示如图 6.14 所示“审核策略更改 属性”对话框。

03 选中“定义这些策略设置”复选框，根据实际需要选择“成功”或“失败”复选框，即可完成该策略的设置。

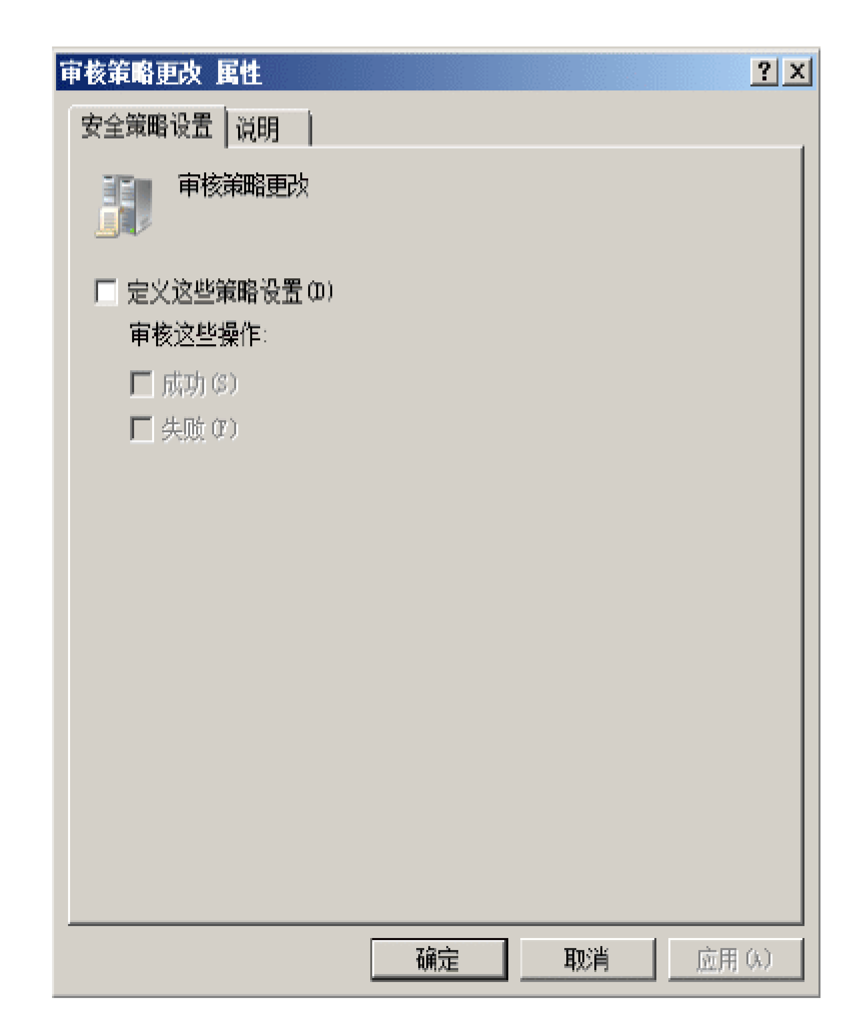


图 6.14 “审核策略更改 属性”对话框

2. 审核登录事件

审核登录事件可以确定是否审核用户登录或注销的每个实例。对于域用户帐户活动，则此事件生成在域控制器上；对于本地帐户活动，则登录事件生成在本地计算机上。

01 依次选择“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“本地策略”→“审核策略”选项，在右侧窗格中双击“审核登录事件”选项，显示如图 6.15 所示“审核登录事件 属性”对话框。

02 选中“定义这些策略设置”复选框，根据实际需要选择“成功”或“失败”复选框，单击“确定”按钮完成该策略的设置。

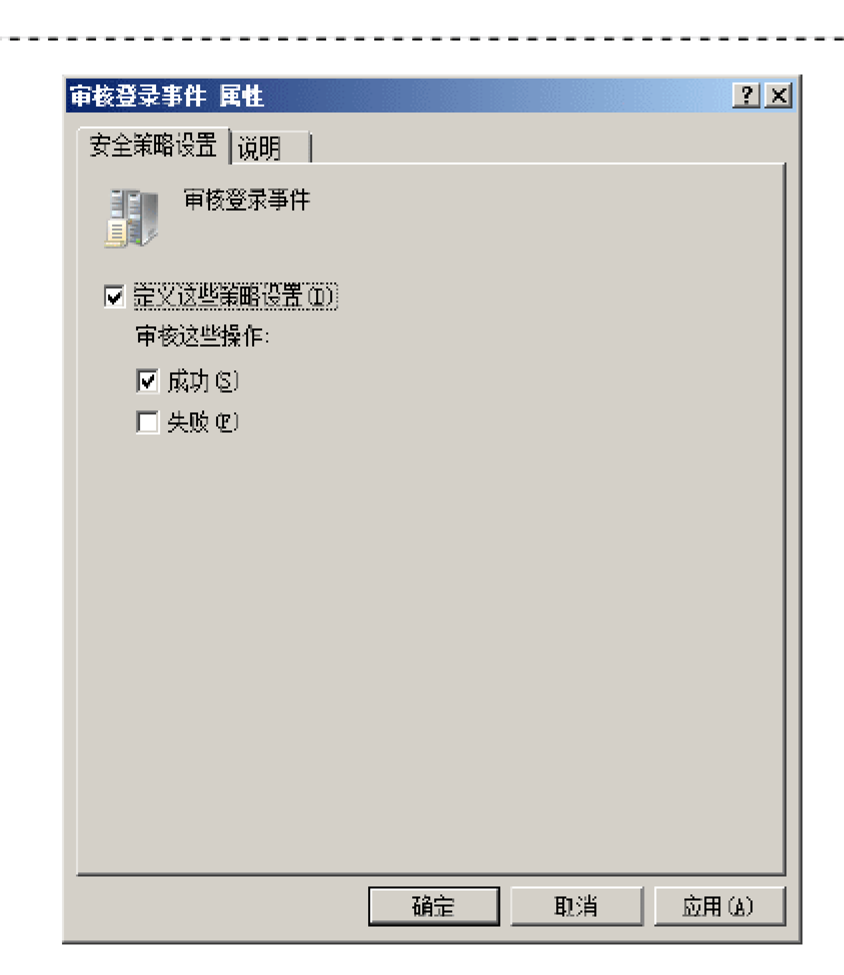


图 6.15 “审核登录事件 属性”对话框

3. 审核对象访问

“审核对象”设置用于确定是否对用户访问指定了自身系统访问控制列表（SACL）的对象（文件、文件夹、注册表和打印机等）这一事件进行审核。如果定义了此策略设置，则可指定是否审核成功、审核失败或根本不审核该事件类型。无论是成功审核还是失败审核都会在用户尝试访问指定 SACL 的对象时生成一个审核项。

01 依次选择“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“本地策略”→“审核策略”选项，在右侧窗格中双击“审核登录事件”选项，显示如图 6.16 所示“审核对象访问 属性”对话框。

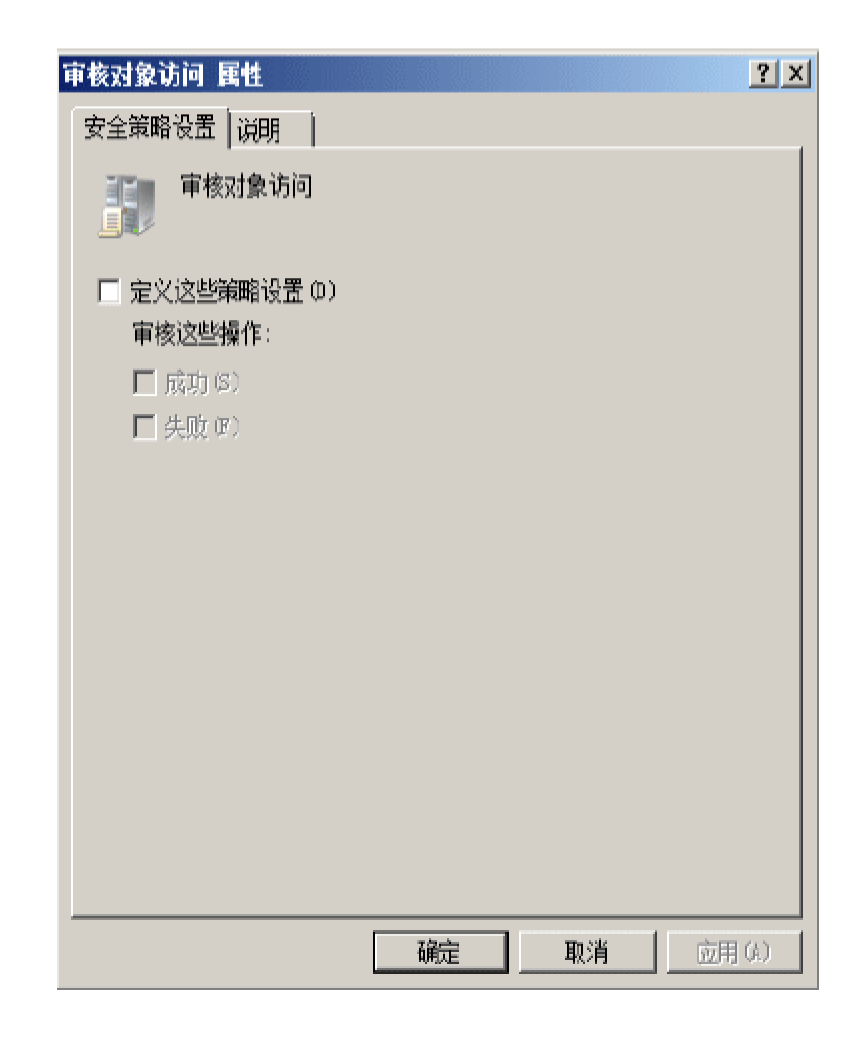


图 6.16　“审核对象访问 属性”对话框

02 选中“定义这些策略设置”复选框，根据实际需要选择“成功”或“失败”复选框，单击“确定”按钮完成该策略的设置。

4．审核进程跟踪

“审核进程跟踪”设置用于确定是否审核事件的详细跟踪信息，如程序的激活、句柄复制、间接对象访问和进程退出等，如果定义了此策略的设置，无论事件审核成功或失败都会在跟踪过程中生成一个审核项。

01 依次选择“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“本地策略”→“审核策略”选项，在右侧窗格中双击“审核进程跟踪”选项，显示如图 6.17 所示“审核进程跟踪 属性”对话框。

02 选中“定义这些策略设置”复选框，根据实际需要选择“成功”或“失败”复选框，单击“确定”按钮完成该策略的设置。

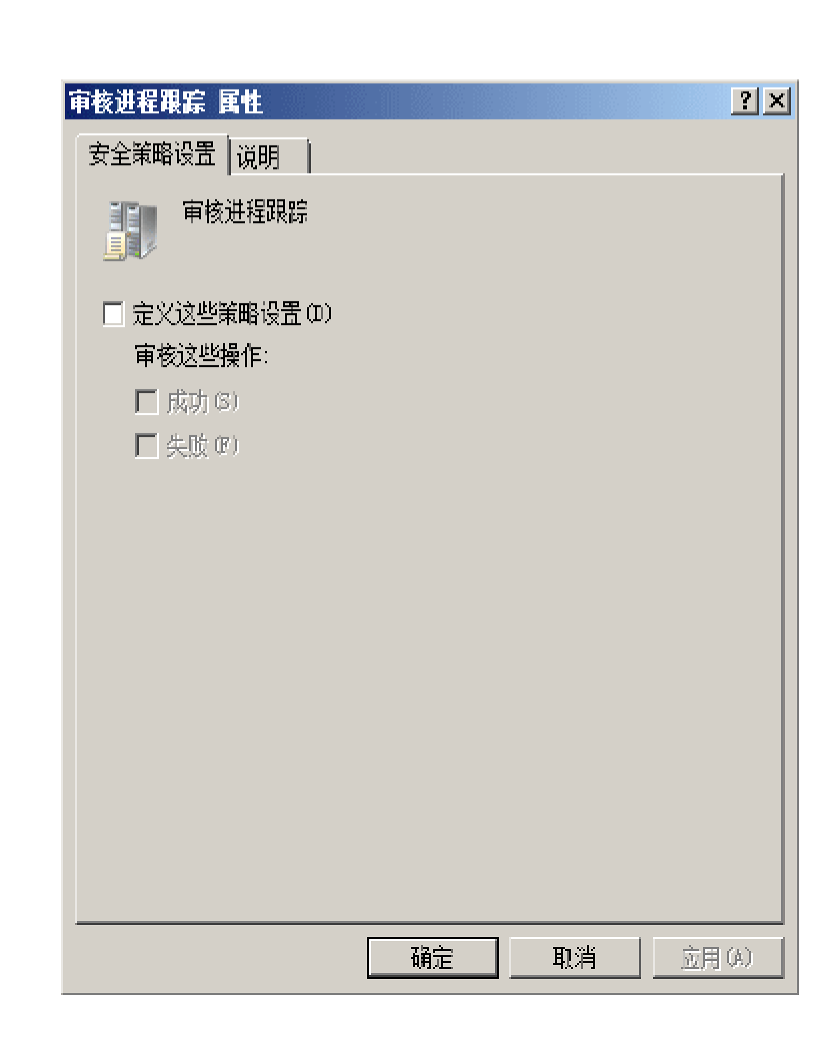


图 6.17　“审核进程跟踪 属性”对话框

5．审核目录服务访问

“审核目录服务访问”设置用于确定是否对用户访问 Active Directory 对象的事件进行审核，该对象指定了自身系统访问控制列表（SACL）。无论用户在成功或失败访问指定了 SACL 的 Active Directory 对象时都会生成一个审核项。

01 依次选择“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“本地策略”→“审核策略”选项，在右侧窗格中双击“审核目录服务访问”选项，显示如图 6.18 所示“审核目录服务访问 属性”对话框。

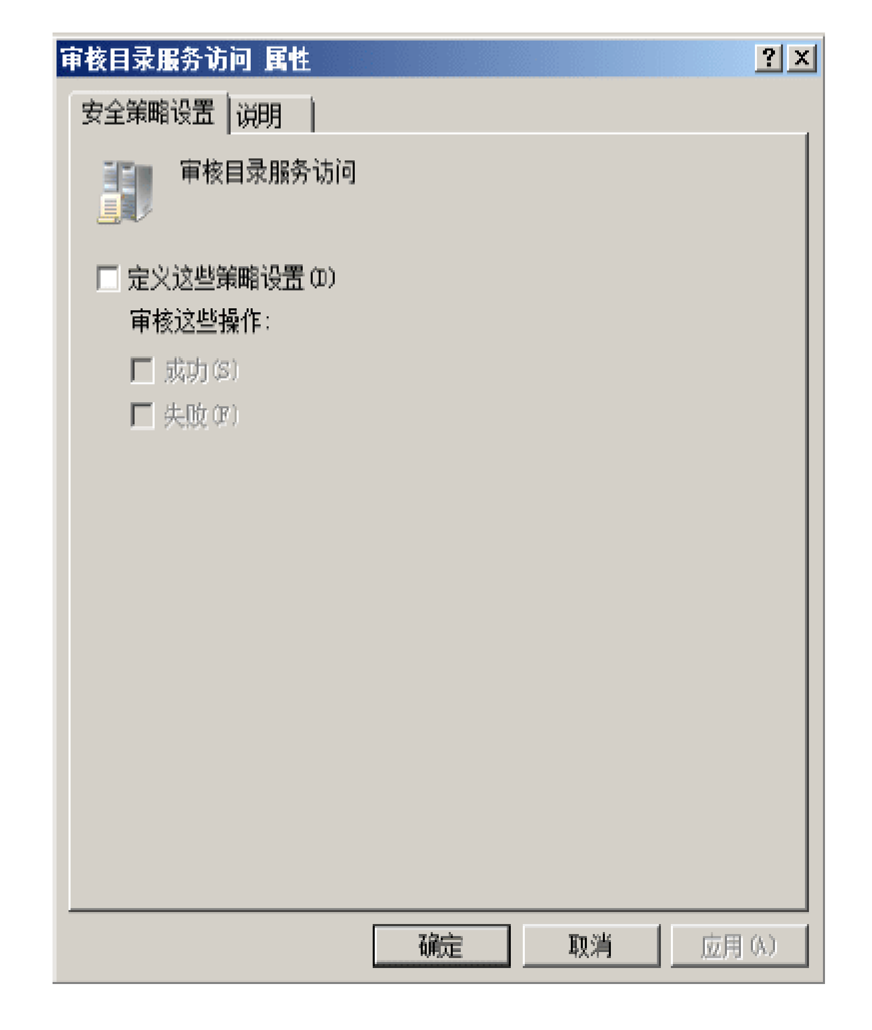


图 6.18 “审核目录服务访问 属性”对话框

02 选中“定义这些策略设置”复选框，根据实际需要选择“成功”或“失败”复选框，单击“确定”按钮即可完成配置。

6. 审核特权使用

“审核特权使用”设置用于确定是否对用户行使用户权限的每个实例进行审核，如果定义了此策略设置，无论是否审核成功或失败，都会生成一个审核项。

01 依次选择“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“本地策略”→“审核策略”选项，在右侧窗格中双击“审核特权使用”选项，显示如图 6.19 所示“审核特权使用 属性”对话框。

02 选中“定义这些策略设置”复选框，根据实际需要选择“成功”或“失败”复选框。默认情况下，即使启用了“审核特权使用”也不会为下列用户权限生成审核事件：

- 跳过遍历检查；
- 调试程序；
- 创建令牌对象；
- 替换进程级令牌；
- 生成安全审核；
- 备份文件和目录；
- 还原文件和目录。

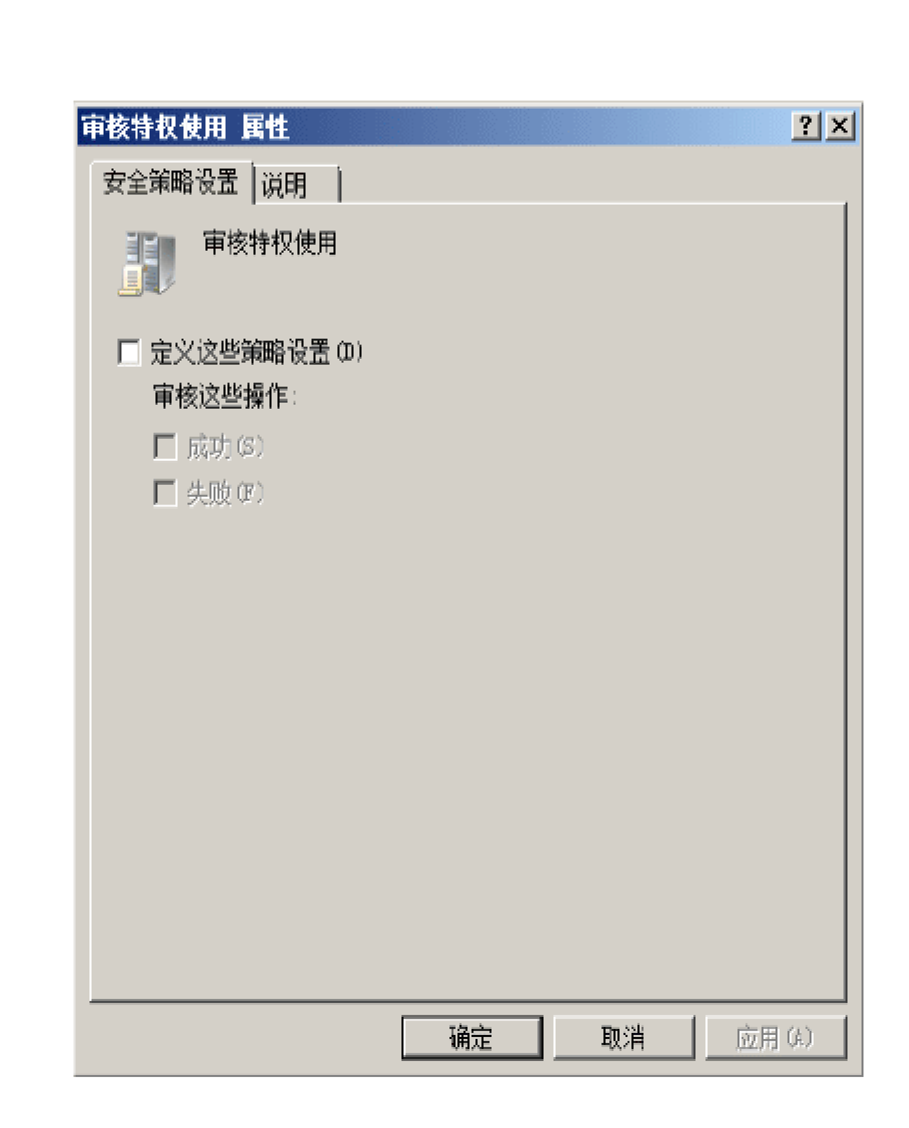


图 6.19 “审核特权使用 属性”对话框

编辑注册表可能严重损坏系统，所以在更改注册表之前，应当备份好计算机上的所有重要数据。

7. 审核系统事件

“审核系统事件”设置用于确定用户重启或关闭计算机时或者发生影响系统安全或安全日志的事件时，是否进行审核。如果定义了此策略设置，无论审核成功或失败都会生成一个审核项。

01 选择“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“本地策略”→“审核策略”选项，在右侧窗格中双击“审核系统事件”选项，显示如图 6.20 所示“审核系统事件 属性”对话框。

02 选中“定义这些策略设置”复选框，根据实际需要选择“成功”或“失败”复选框，单击“确定”按钮即可完成设置。

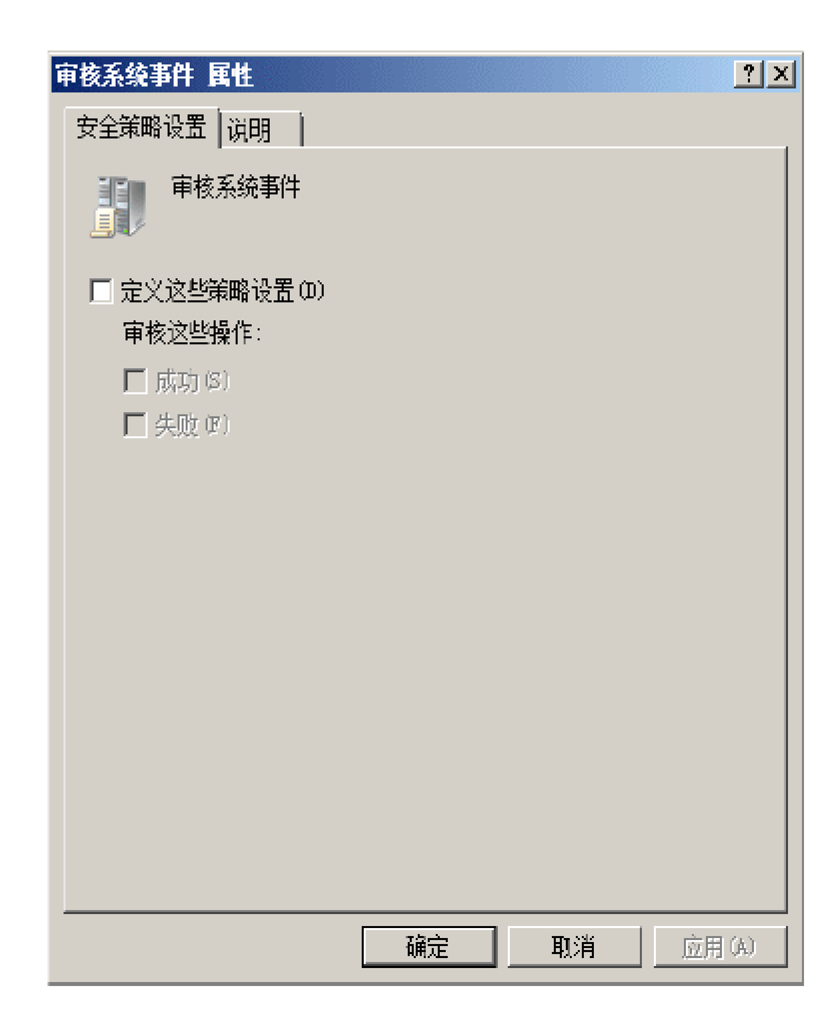


图 6.20　“审核系统事件 属性”对话框

8. 审核帐户登录事件

“审核帐户登录事件”设置用于确定是否对用户在另一台计算机上登录或注销的每个实例进行审核。如果定义了此策略设置，无论审核成功或失败都会生成一个审核项。如果在域控制器上启用了帐户登录事件的成功审核，则对于没有通过域控制器验证的每个用户，都会生成一个审核项，即使该用户实际上只是登录到加入该域的一个工作站上。

01 依次选择“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“本地策略”→“审核策略”选项，在右侧窗格中双击“审核帐户登录事件”选项，显示如图 6.21 所示“审核帐户登录事件 属性”对话框。

02 选中“定义这些策略设置”复选框，根据实际需要选择“成功”或“失败”复选框，单击“确定”按钮即可完成设置。

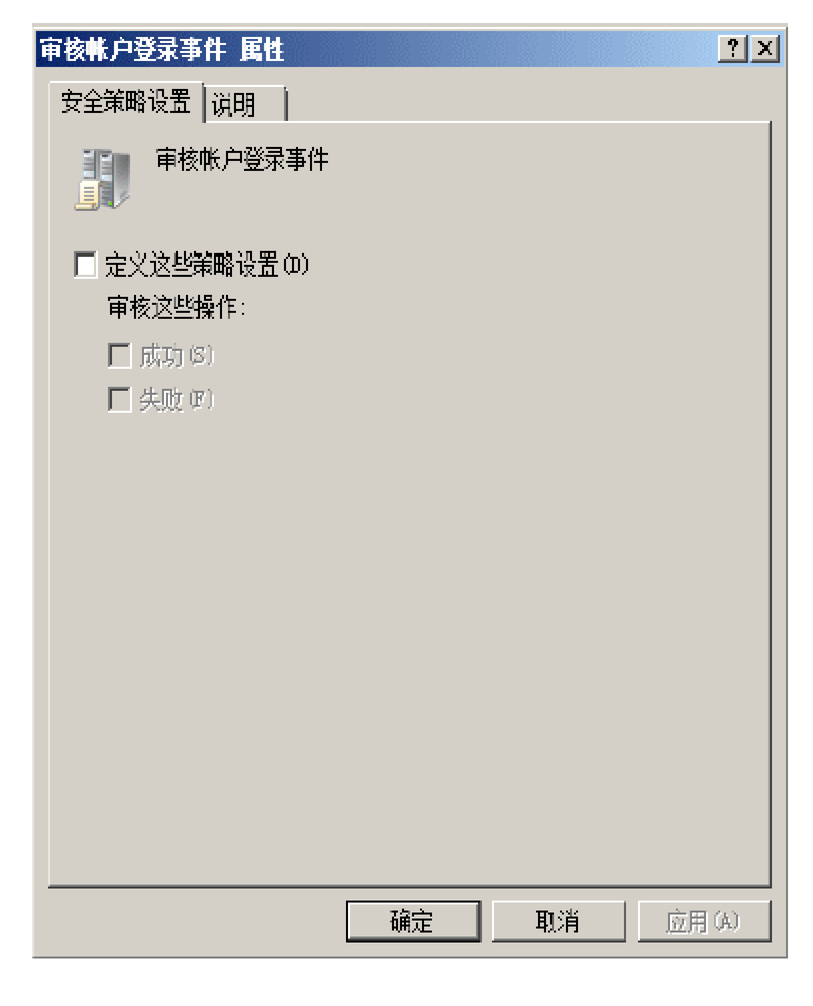


图 6.21　“审核帐户登录事件 属性”对话框

9. 审核帐户管理

“审核帐户管理”设置用于确定是否对计算机上的每个帐户管理时间进行审核。帐户管理事件示例包括：

- 创建、修改或删除用户帐户或组；
- 重命名、禁用或启用用户帐户；
- 设置或修改密码。

如果定义了此策略设置，无论审核成功或失败都会生成一个审核项。在响应安全事件时，阻止对创建、更改或删除帐户的人员进行跟踪。

01 依次选择“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“本地策略”→“审核策

略”选项，在右侧窗格中双击“审核帐户管理”选项，显示如图 6.22 所示“审核帐户管理 属性”对话框。

02 选中“定义这些策略设置”复选框，然后根据实际需要选择“成功”或“失败”复选框，单击“确定”按钮即可完成设置。

图 6.22 “审核帐户管理 属性”对话框

6.3.3 证书规则限制策略

使证书与软件进行绑定，当软件在网络上运行时通过对证书的验证也已确认该软件是否是合法软件，从而提高网络环境的安全性。

1. 软件限制策略

使用“软件限制策略”，通过标识并指定允许哪些应用程序运行，可以保护用户的计算机免受不可信任的代码的侵扰。

01 在“组策略管理器”中，依次选择“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“软件限制策略”选项，打开“组策略管理编辑器”窗口。右击“其他规则”选项，在弹出的快捷菜单中选择“新建证书规则”命令，显示如图 6.23 所示“新建证书规则”对话框。

02 单击“浏览”按钮，显示如图 6.24 所示“打开”窗口，选择相关证书单击“确定”按钮，返回到“新建证书规则”对话框。



图 6.23 新建证书规则

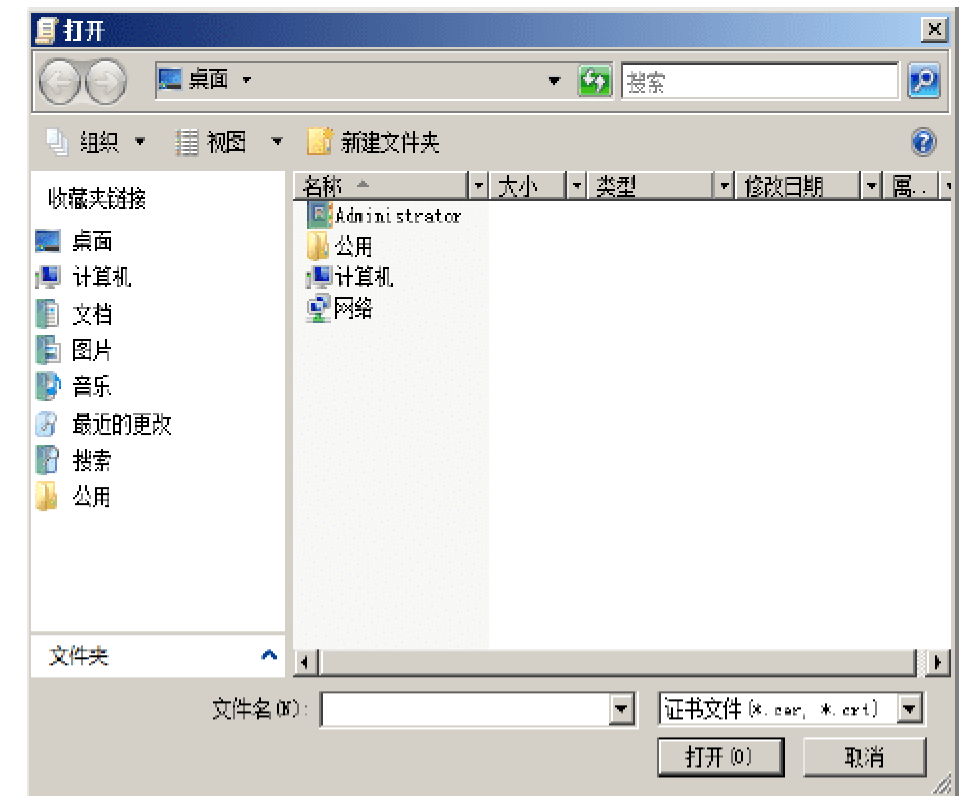


图 6.24 “打开”窗口

03 在“安全级别”下拉列表项中选择“不允许”选项，单击“确定”按钮，显示如图 6.25 所示“软件限制策略”对话框。

04 单击“是”按钮，显示如图 6.26 所示“强制 属性”对话框，根据实际情况选择该证书限制的文件、用户证书的执行状态。

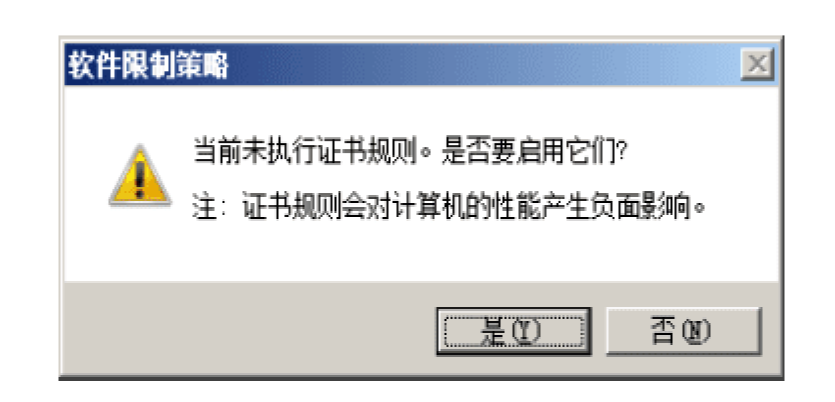


图 6.25　“软件限制策略”对话框

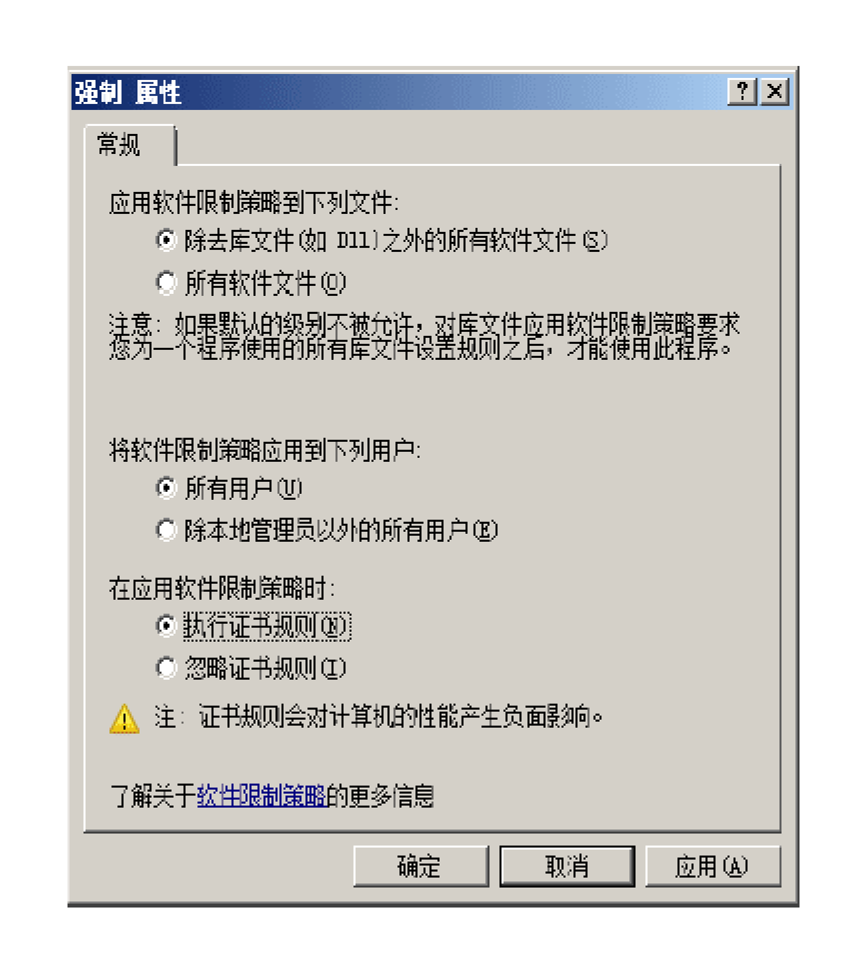


图 6.26　“强制 属性”对话框

05 依次单击“确定”按钮完成证书规则的创建。

2. 客户端测试

当客户端计算机运行“qq.exe”时，显示如图 6.27 所示“此程序被组策略阻止”对话框。

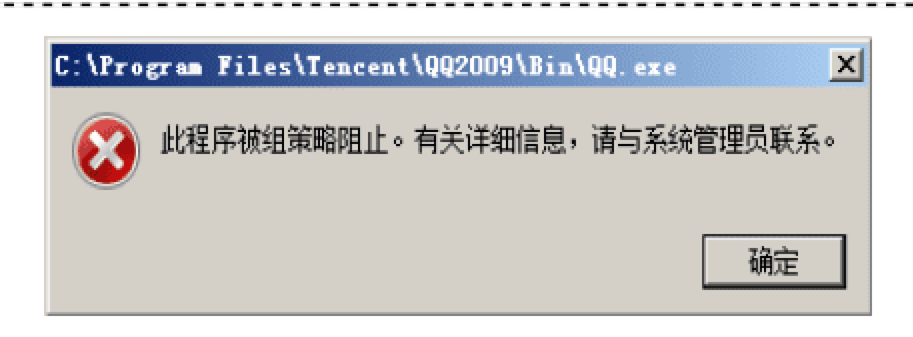


图 6.27　“此程序被组策略阻止”对话框

6.4　软件限制策略

软件限制策略的主要功能在于控制未知或不信任的软件安装，如间谍软件、恶意程序等。使用组策略的软件限制策略功能，可以为策略作用域下用户的软件使用进行限制。顾名思义，软件限制策略就是限制某些软件的使用。使用组策略的限制软件策略，可以通过规则标识并设置安全级别来指定软件是否运行从而达到客户端计算机系统的可管理性、安全性。使用目的是控制不信任的和不被允许的软件在网络内的非法使用，例如使用软件限制策略可以禁止运行 QQ、MSN 等聊天工具。

6.4.1　软件限制策略概述

使用软件限制策略，可通过标识并指定允许运行的软件来保护计算机环境免受不信任软件的侵袭。可以为组策略对象定义“不受限的”或“不允许的”的默认安全级别，从而决定是否在默认情况下允许软件运行。通过为特定软件创建软件限制策略规则，可以相对于默认安全级别做出例外安排。软件限制策略使用规则来标识和控制软件的运行方式。可以通过软件程序的哈希、证书、路径或其所驻留的 Internet 区域对其进行标识。对软件进行了标识后，可以决定是否允许运行。

软件限制策略可应用于计算机或用户，这取决于是修改“计算机配置”中的设置还是“用户配置”中的设置。软件限制策略是通过组策略得以应用的。需要将策略设置应用于组策略对象，该对象与本地计算机、站点、域或组织单位相连。如果应用了多个策略设置，将遵循以下优先级顺序（从低到高）：

- 本地计算机策略；
- 站点策略；
- 域策略；
- 组织单位策略。

所有策略设置在重新启动计算机后都会被刷新。修改策略设置时，在工作站或服务器上每 90 分钟刷新一次，而在域控制器上每 5 分钟刷新一次。不管是否更改了策略设置，它们都会每 16 小时刷新一次。通过先运行强制刷新组策略命令 gpupdate /force，然后注销计算机并重新登录来刷新策略设置。

软件限制策略中的规则标识一个或多个应用程序，以指定是否允许其运行。

软件限制策略使用下列 4 个规则来标识软件：

- 哈希规则：使用可执行文件的加密密钥；
- 证书规则：用软件发布者为 .exe 文件提供的数字签名证书；
- 路径规则：使用 .exe 文件位置的本地路径、通用命名约定（UNC）路径或注册表路径；
- 区域规则：使用可执行文件源自的 Internet 区域。

使用软件限制策略可以实现以下目的：

- 控制软件在系统中的运行能力；
- 允许用户在多用户计算机上仅运行特定文件；
- 决定可以在计算机中添加信任的发布者的用户；
- 控制软件限制策略是作用于所有用户，还是仅作用于计算机上的某些用户；
- 阻止任何文件在本地计算机、组织单位、站点或域中运行。

6.4.2 部署基本策略

Windows Server 2008 组策略中提供了简单的软件限制策略“不要运行指定的 Windows 应用程序”，可以对应用程序进行限制。

1. 策略部署

限制 Default Domain Policy 中的用户使用 QQ。

---

01 打开“组策略管理”窗口，选择“林：corp.contoso.com”→“corp.contoso.com”→“company”选项。右击“company”选项，在弹出的快捷菜单中选中“在这个域中创建 GP0 并在此链接”命令，显示如图 6.28 所示“新建 GP0”对话框，在“名称”文本框中输入新建的名称。单击“确定”按钮，创建新的组策略对象。

02 右击“软件限制策略”选项，在弹出的快捷菜单中选择“编辑”命令，打开“组策略管理编辑器”窗口。依次选择“用户配置”→“策略”→“管理模板”→“系统”选项，显示如图 6.29 所示“系统设置”窗口。

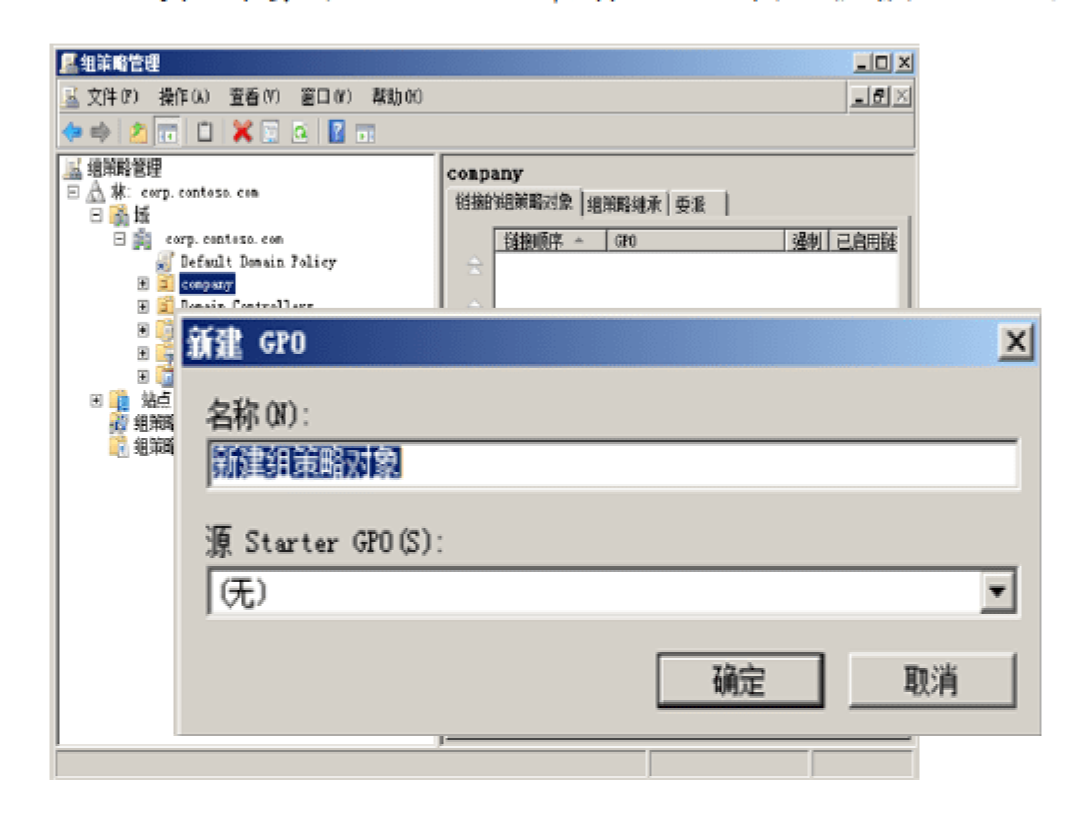


图 6.28　“新建 GP0”对话框

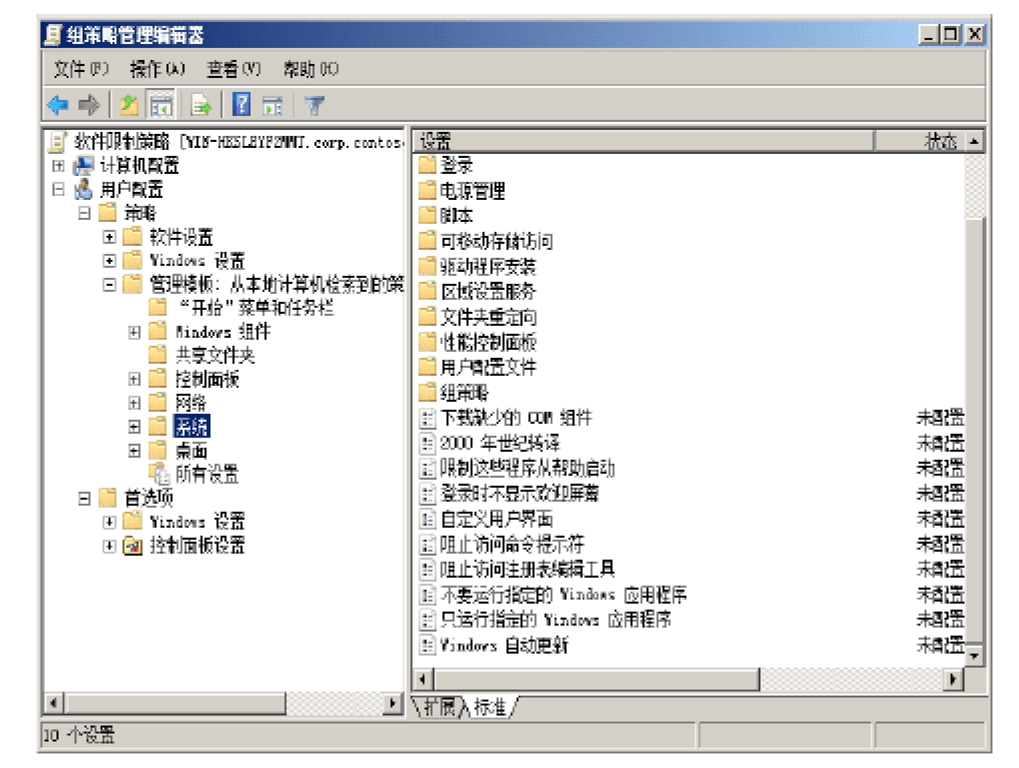
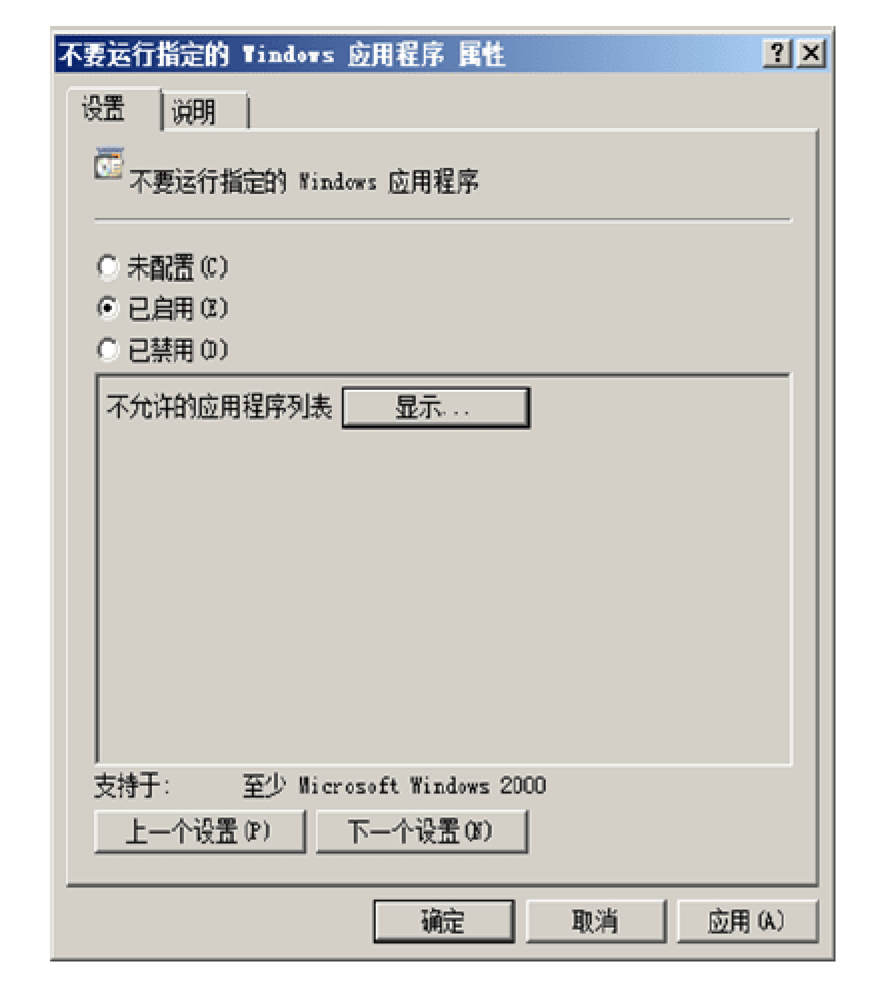


图 6.29　“系统设置”窗口

03 在右侧窗格中双击“不要运行指定的 Windows 应用程序”选项，显示如图 6.30 所示“不要运行指定的 Windows 应用程序 属性”对话框。选中“已启用”单选按钮，单击“显示”按钮，显示“显示内容”对话框。单击“添加”按钮，显示“添加项目”对话框，在“输入要添加的项目”的文本框中输入“qq.exe”。



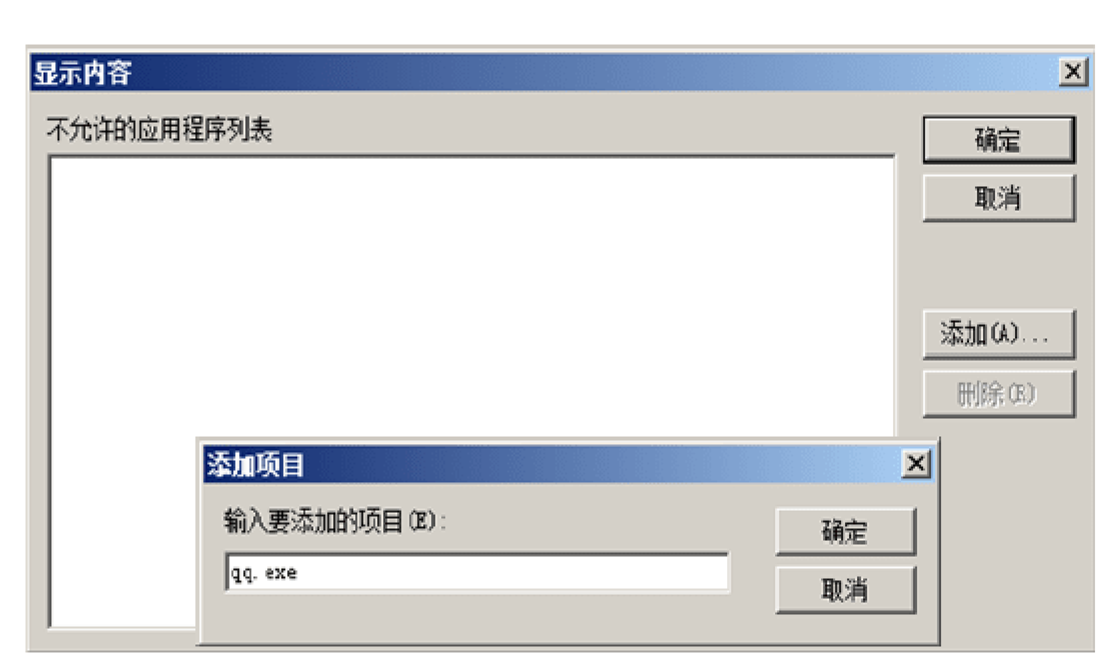


图 6.30　设置不要运行的 Windows 应用程序

04 依次单击“确定”按钮，保存设置即可。

2. 客户端测试

在客户端计算机上，双击“qq2009.exe”应用程序，显示如图 6.31 所示“限制”对话框。

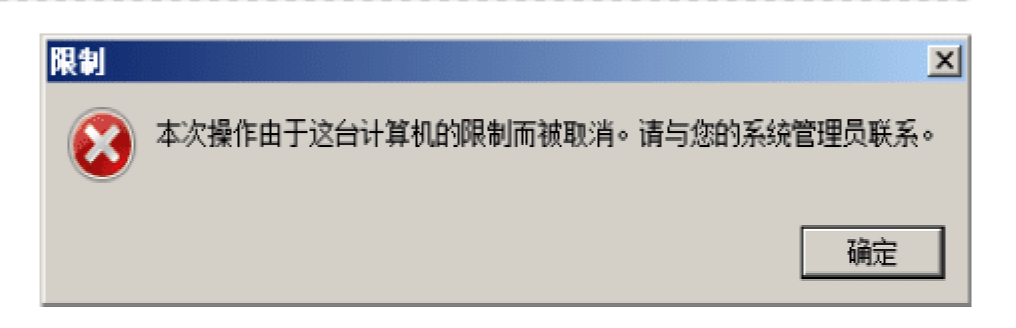


图 6.31　“限制”窗口



注意　如果应用程序文件改名，那么该限制策略将失效。这个策略仅防止用户运行 Windows 资源管理器启动的程序，不能阻止用户运行系统过程或其他过程的哪个程序，如任务管理器。

如果允许用户访问命令提示符 Cmd.exe，那么这个设置不能阻止用户在命令窗口启动该策略限制的应用程序。

6.4.3 哈希规则策略

哈希值是根据文件内容的数据通过逻辑运算得到的数值，它能把一些不同长度的信息转化为杂乱的 128 位编码，是一种加密算法。为软件指定哈希规则后，软件限制策略会自动为指定软件计算一个哈希值，当用户使用该软件时，客户端操作系统会将该软件的哈希值与软件限制策略已有的哈希值进行比较，如果值相同则该软件允许运行。

1. 策略部署

01 在“组策略管理器”中，依次展开“计算机配置”→“Windows 设置”→“安全设置”→“软件限制策略”，右击“软件限制策略”，在弹出的快捷菜单中选择“创建软件限制策略”选项如图 6.32 所示“组策略管理编辑器”窗口。

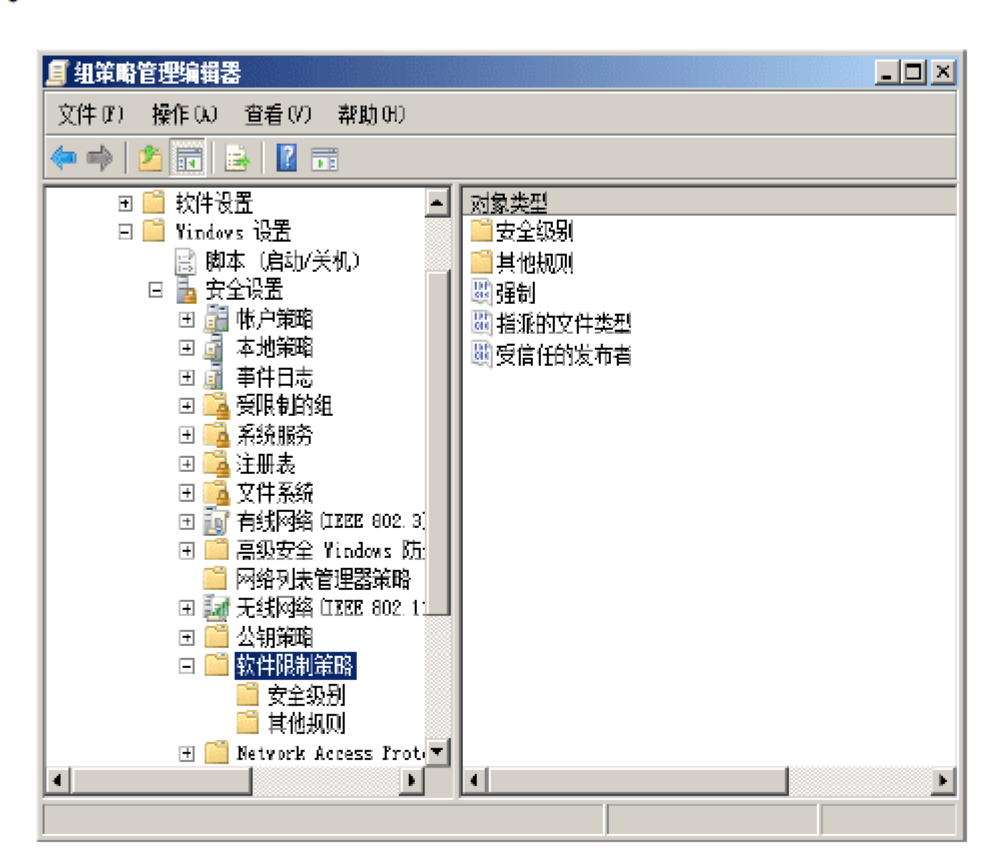


图 6.32 “组策略管理编辑器”窗口

02 右击“其他规则”在弹出的快捷菜单中选择“新建哈希规则”选项，显示如图 6.33 所示“新建哈希规则”对话框。单击“浏览”按钮，选择需要限制的程序，例如“QQ.exe”。

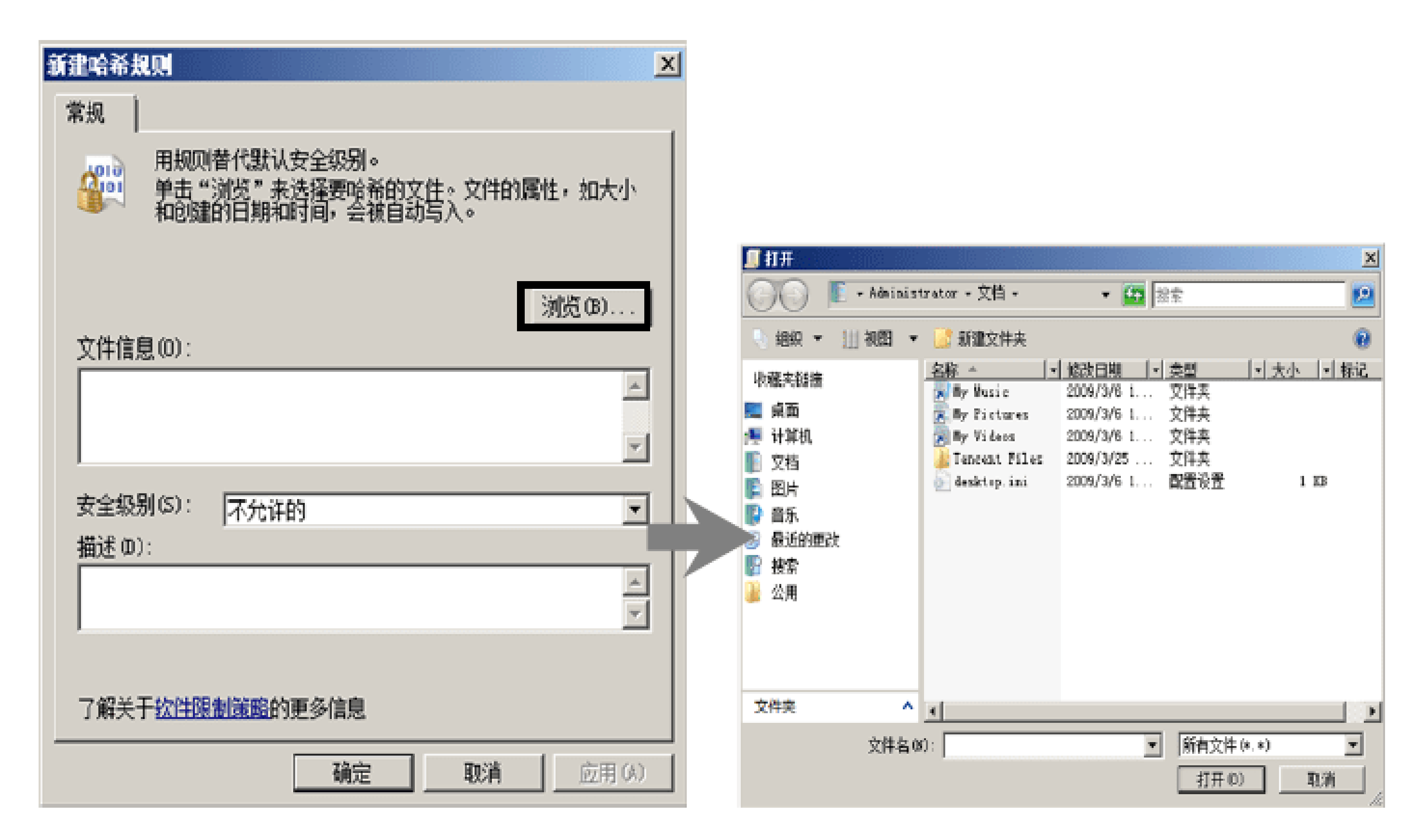


图 6.33 新建哈希规则

03 单击“确定”按钮，返回“新建哈希规则”对话框，在“安全级别”下拉列表框中选择“不允许的”选项，表示不允许运行此程序，如图 6.34 所示。

04 单击“确定”按钮，完成该策略配置，显示如图 6.35 所示“组策略管理编辑器”窗口。

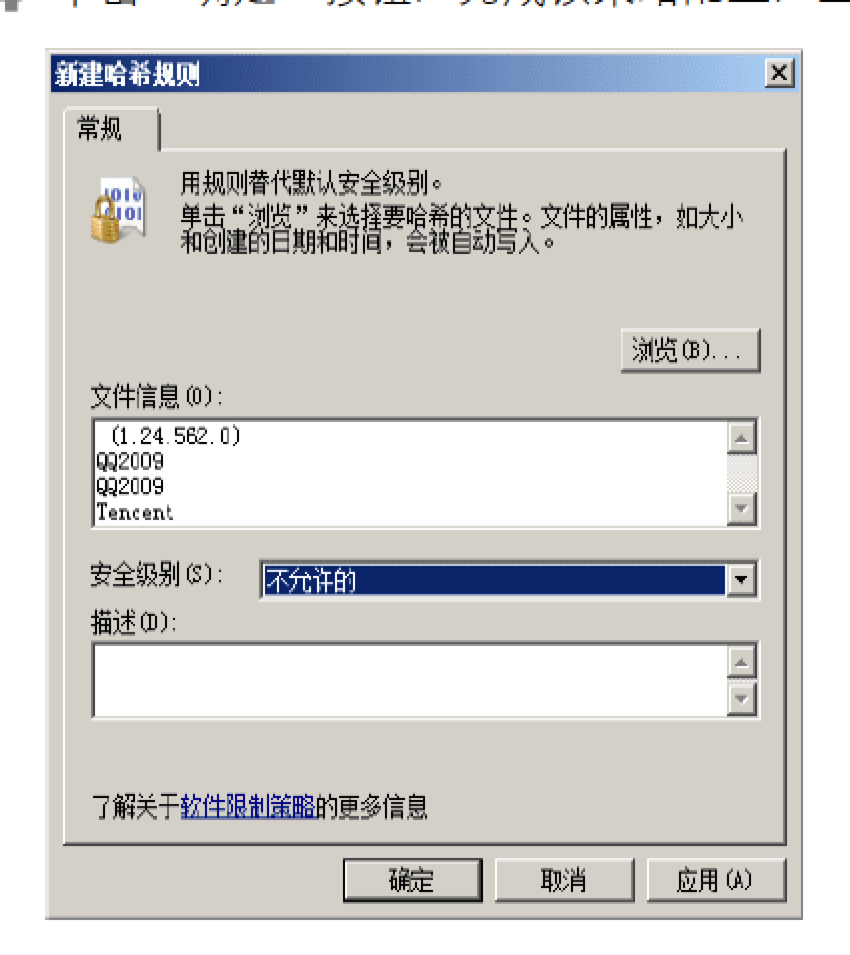


图 6.34　设置完成的“新建哈希规则”对话框

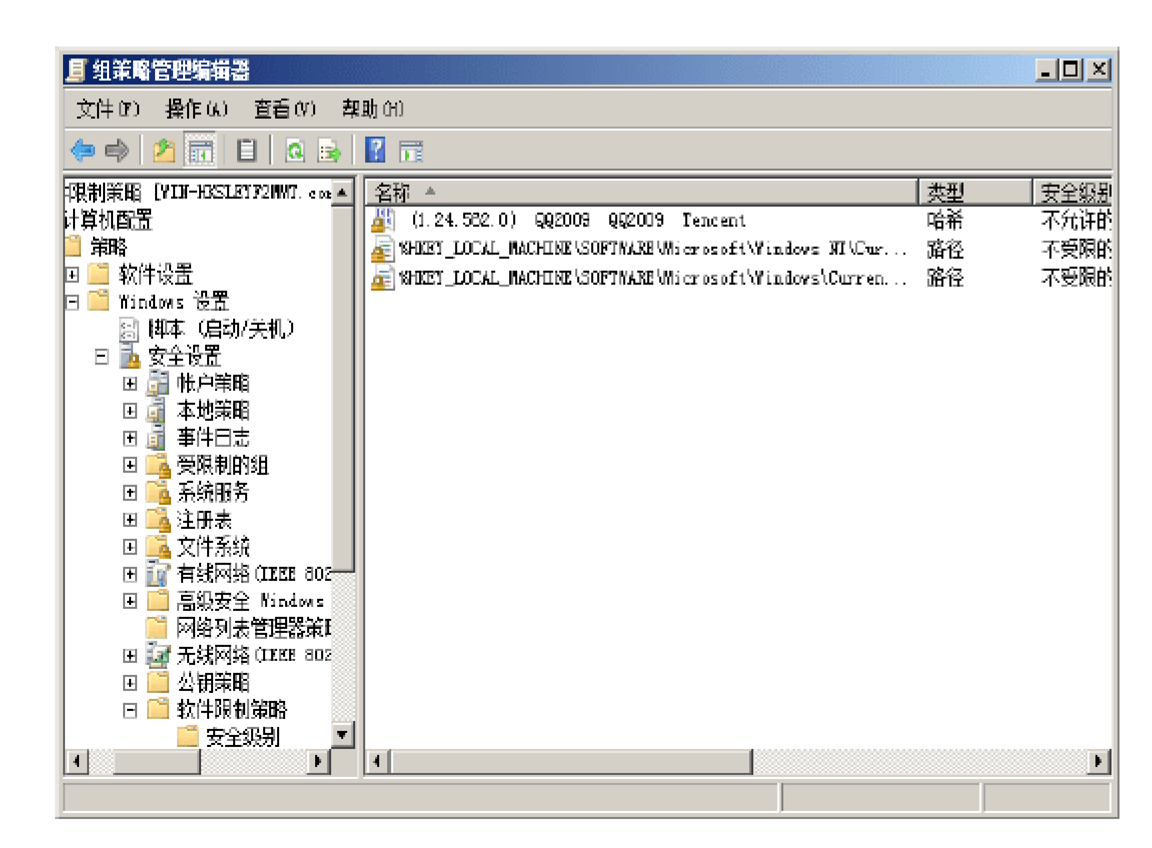


图 6.35　“组策略管理编辑器”窗口

2. 客户端测试

在客户端计算机运行 QQ.exe 时，显示如图 6.36 所示“此程序被组策略阻止”对话框，表明软件限制策略已经生效。

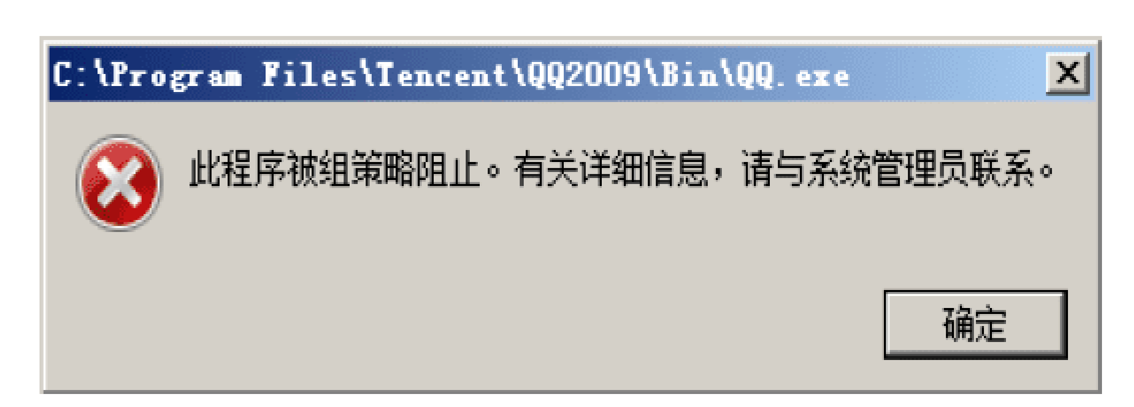


图 6.36　“此程序被组策略阻止”对话框

6.5　硬件限制策略

现在移动存储设备越来越普及，通过其所传播的病毒，也给网络管理员带来新的难题。Windows Server 2008 通过组策略即可控制对移动设备的访问以及硬件设备的安装，从而阻止病毒或恶意软件通过移动存储设备传播和安装。

01 将任意 U 盘插入计算机的 USB 接口，打开“计算机管理”→“设备管理器”窗口，展开“磁盘驱动器”选项，显示如图 6.37 所示窗口。

02 右击 U 盘对应的设备名称，选择“属性”选项，在打开对话框中单击“详细信息”，切换至如图 6.38 所示“详细信息”选项卡。在“属性”下拉列表中选择“设备类 GUID”选项，在“值”列表中，显示的就是 U 盘类设备对应的 GUID，将此值复制到粘贴板即可。单击“确定”按钮，关闭对话框。



图 6.37 “计算机管理”窗口

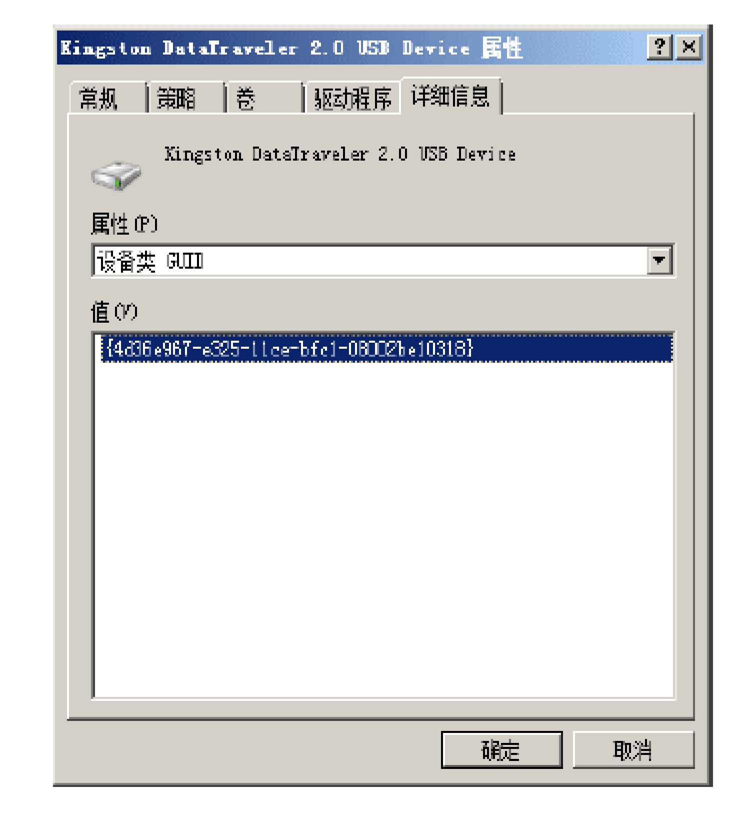


图 6.38 “详细信息”选项卡

03 在组策略管理器窗口中，依次展开“计算机配置”→“管理模板”→“系统”→“设备安装”→“设备安装限制”分支，双击“阻止安装与下列任何设备 ID 相匹配的设备”策略，显示策略属性对话框，选择“已启用”单选按钮。单击“显示”按钮，显示“显示内容”对话框，默认此列表为空白。单击“添加”按钮，显示“添加项目”对话框，将复制到粘贴板的 U 盘类设备 GUID，粘贴到“输入要添加的项目”文本框中即可，如图 6.39 所示。

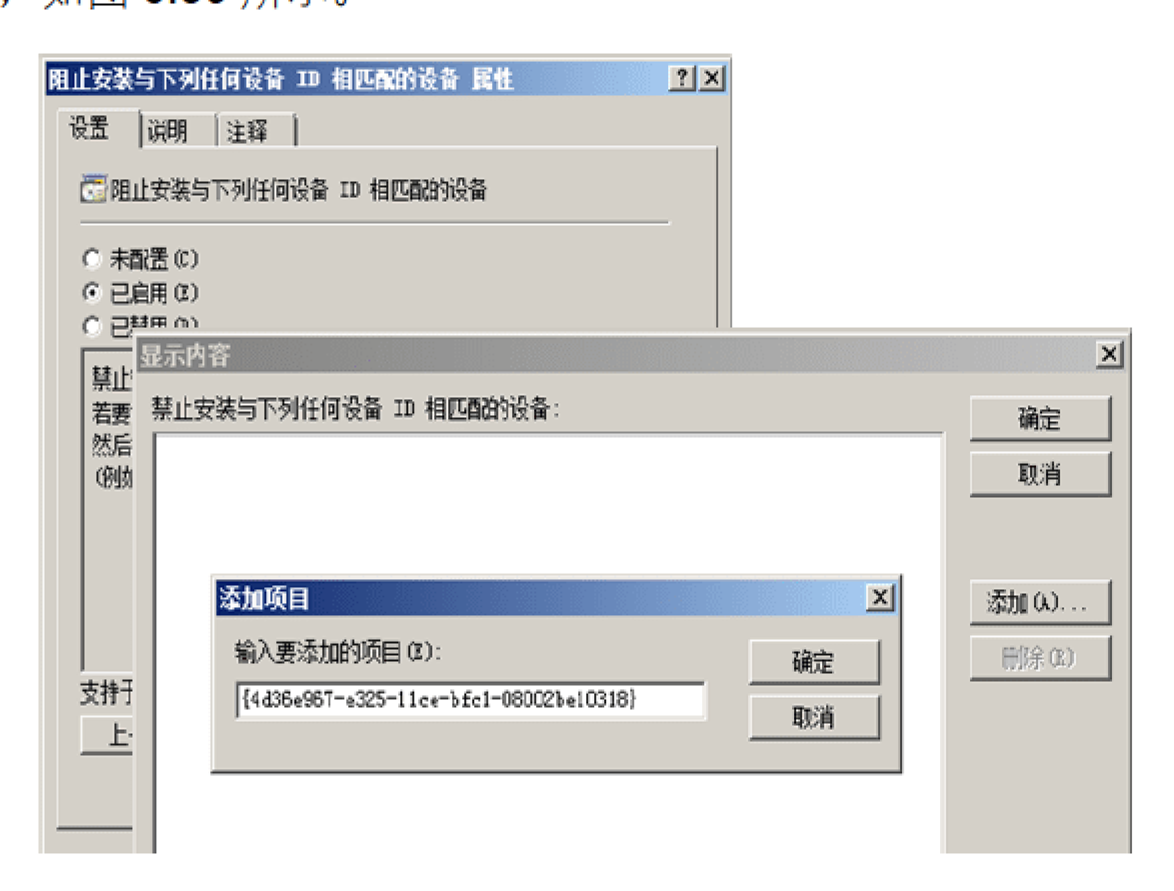


图 6.39 设置硬件访问控制策略

04 依次单击“确定”按钮，保存设置即可。由于以上策略只是阻止使用 U 盘类设备，所以应用此策略后，用户仍可以将 U 盘插入 USB 接口，并且系统会自动为其安装驱动程序，但是在资源管理器中打开时，会发现 U 盘对应的可用磁盘空间为 0，不会显示任何数据。

这些措施，并不能从根本上解决核心数据的安全问题。恶意用户仍然可以通过电子邮件发送数据，并且如果是管理员的话，具备工作站或服务器的物理操作权限，则盗取数据更是易如反掌。所以说，最完美的解决方案是确保核心数据的访问权限，而不是仅仅依靠组策略。

注意  如果在应用设备限制策略之前，用户已经将移动设备安装到系统中，则不能阻止用户的正常应用，该策略会在用户取下设备并再次安装移动设备时生效。

小　　结

本节主要在域环境下讲解组策略安全，通过组策略可以控制应用程序、设置系统环境和管理模板，方便管理员对企业网络的管理，如部署软件、设置硬件访问策略、定制用户环境等，这些都大大提高了网络的安全性。

习　　题

1. 组策略有哪些实用功能？
2. 系统默认的组策略模板有哪些，分别有哪些功能？
3. 计算机配置策略和用户配置策略有何区别？
4. 本地安全策略和组策略管理编辑器有何区别？

实验：配置用户帐户锁定策略

实验目的

掌握如何通过限制用户登录重试次数，保护系统安全。

实验内容

在 Windows Server 2008 域控制器的默认域策略中，编辑帐户锁定策略，用户登录时重试次数超过 3 次即被锁定。

实验步骤

1. 打开“组策略管理编辑器”窗口，编辑默认域策略。
2. 编辑帐户锁定策略中的“帐户锁定阈值”，设置为 3。
3. 使用测试用户帐户，验证策略有效性。
4. 将策略应用到所有域用户。



第7章

数据存储安全

Internet 技术及其相关应用极大推动了信息化的普及，企业和组织机构内部的信息系统建设已初具规模，包括企业员工的 PC、服务器到数据中心。随之而来网络中大量数据信息的安全问题，像自然灾害、硬件设备故障、网络攻击、管理不当、误操作等都可能导致重要信息的丢失，随时可能使企业蒙受巨大的经济损失。为此，各种安全存储技术不断涌现，一场没有硝烟的数据安全保卫战正在展开。

本章导读

- 磁盘配额
- 数据备份与恢复
- 软件 RAID

7.1　磁盘配额

在 Windows Server 2008 为服务器操作系统的计算机网络中，系统管理员有一项很重要的任务，即用户设置磁盘配额，也就是限制其使用服务器空间数量，目的在于防止个别用户滥用服务器和网络资源，确保为所有用户合理分配服务器存储空间。

7.1.1　磁盘配额的功能

磁盘配额管理技术，主要是根据网络管理员设置的标准，跟踪对被保护卷的写入操作，如果被保护卷达到或超过了设定级别，则用户就会收到服务器自动发送的消息，警告该卷已经接近配额，或者磁盘配额管理器将阻止用户向该卷写入数据。管理员能够启用磁盘配额，并设置两个值：

- 磁盘配额限度。用于指定允许用户使用的磁盘空间容量；
- 磁盘配额警告级别。指定了用户接近其配额限度的值。

在 Windows Server 2008 系统中，管理员可以配置当用户超过所指定的磁盘空间限额时，阻止其进一步使用磁盘空间和记录事件，或当用户超过指定的磁盘空间警告级别时，记录事件。第一种配置情况下，用户在使用磁盘时如果超过指定的磁盘空间，将无法使用；第二种情况允许用户超额使用磁盘，但会将此情况记录在事件中。

同时可以指定用户能超过其配额限度。如果不想拒绝用户访问卷但想跟踪每个用户的磁盘空间使用情况，启用配额但不限制磁盘空间使用将非常有用。也可指定不管用户超过配额警告级别还是超过配额限度时是否记录事件。

启用卷的磁盘配额时，磁盘配额不应用到现有的卷用户上。可以通过在“配额项目”窗口中添加新的配额项目将磁盘空间配额应用到现有的卷用户上。

由于磁盘配额能够监视单个用户的卷使用情况，因此每个用户对磁盘空间的利用都不会影响同一卷上的其他用户的磁盘配额。在用户看来与在一个独立的磁盘卷中进行操作没什么两样。

要支持磁盘配额，磁盘卷必须使用 NTFS 文件系统格式化，且不受卷中用户文件的文件夹位置的限制。

7.1.2　磁盘配额管理

如果要在已经使用的磁盘中启用磁盘配额功能，Windows Server 2008 将计算到启动时间点为止，在该卷中复制文件、保存文件或取得文件所有权的所有用户，使用的磁盘空间。根据统计结果，自动为每个用户设置配额限度和警告级别。当然，管理员可以为某个或多个用户设置不同的配额或禁用配额。另外，也可以为还没有在卷上复制文件、保存文件或取得文件所有

权的用户设置磁盘配额，或者在一个新创建的卷上启用磁盘配额功能。

使用磁盘配额过程中，应注意以下 2 个方面：

- 驱动器的文件格式必须为 NTFS 文件系统格式。如果驱动器的磁盘格式为 FAT32 文件系统，可以使用 Windows Server 2003/2008 提供的文件系统转换工具 Convert 进行转换；
- 必须以管理员或管理员组成员的身份登录到 Windows 系统。

在文件服务器上选中“为此服务器的新用户设置默认磁盘空间配额”复选框，在“将磁盘空间限制为”和“将警告级别设置为”文本框中，输入适当的数值，使用户只能使用规定数额的磁盘空间，从而避免服务器硬盘的滥用。当用户使用的空间达到指定的警告值时，系统将提示用户磁盘空间剩余值。当用户使用的空间达到规定的磁盘限额时，系统将禁止用户再向服务器写入文件，从而确保服务器硬盘空间被合理、公平的使用。

1. 启动磁盘限额

在默认的情况下，磁盘配额是没有启用的。启动磁盘配额的操作步骤如下：

01 在 Windows 资源管理器中，右击“本地磁盘（D:）”盘符选项，选择快捷菜单中的“属性”命令，显示“本地磁盘（D:）属性”对话框，切换到如图 7.1 所示“配额”选项卡，选中“启用配额管理”复选框，即可启用磁盘配额管理。选择其中相应的各个选项，以配置系统的磁盘配额功能：

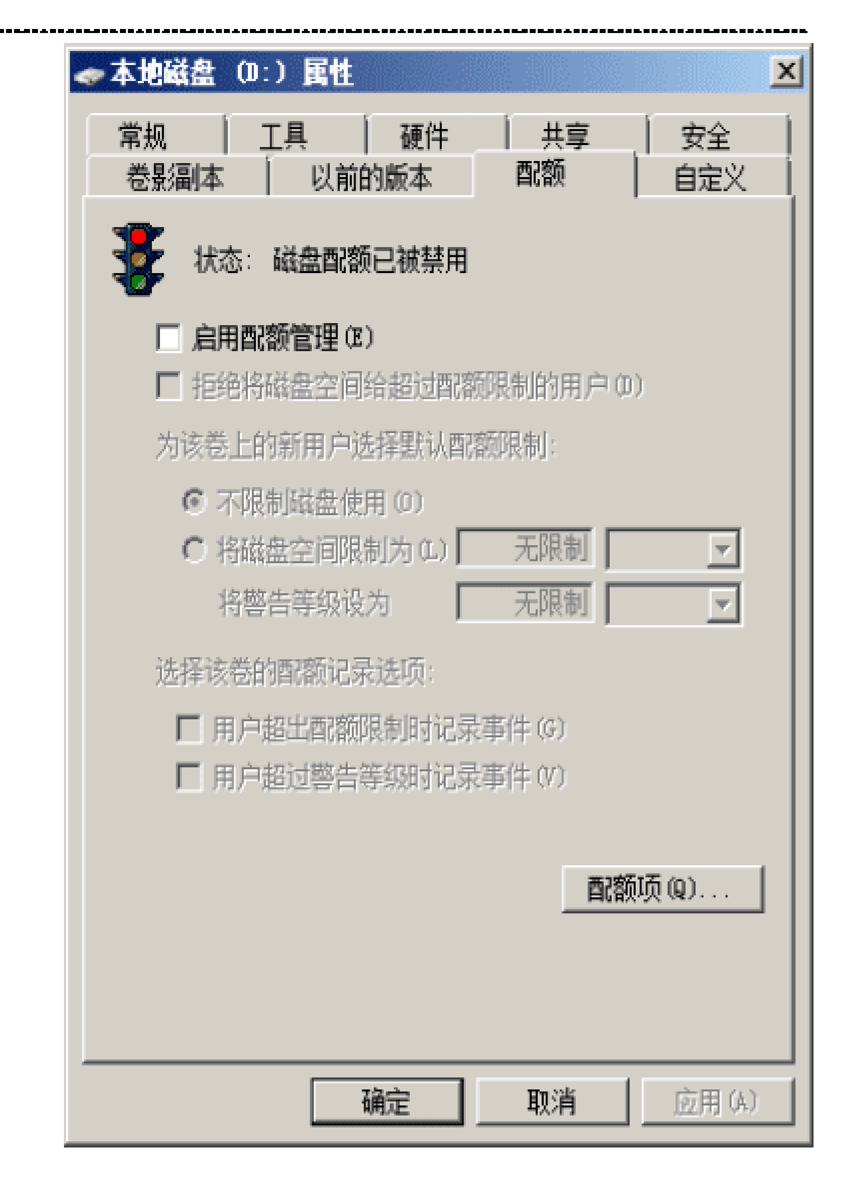


图 7.1 “配额”选项卡

- 选中“拒绝将磁盘空间给超过配额限制的用户”复选框，超过其配额限制的用户，将收到来自 Windows 的“磁盘空间不足”的错误信息，并且在没有从中删除和移动一些现存文件的情况下，无法将额外的数据写入卷中。如果取消该复选框，则用户可以超过其配额限制；
- 选中“将磁盘空间限制为” 单选按钮，并输入允许卷的新用户使用的磁盘空间数量，以及在将事件写入系统日志前已经使用的磁盘空间量。网络管理员可以在“事件查看器”中查看这些事件。在磁盘空间和警告级别中可以使用十进制数值，从下拉列表中选择适当的单位（如 KB、MB、GB 等）；
- 选中“用户超出配额限制时记录事件”复选框。此时如果启用配额，则只要用户超过其配额限制，事件就会写入到本地计算机的系统日志中。管理员可以用“事件查看器”，通过筛选磁盘事件类型来查看这些事件。默认情况下，配额事件每小时都会被写入本地计算机的系统日志中；
- 选中“用户超过警告等级时记录事件”复选框。此时如果启用配额，则只要用户超过其警告级别，事件就会写入到本地计算机的系统日志中。管理员可以用事件查看器，通过筛选磁盘事件类型来查看这些事件。默认情况下，配额事件每小时都会被写入本地计算机的系统日志中。

02 单击“确定”按钮，保存所做设置，启用磁盘配额完成。

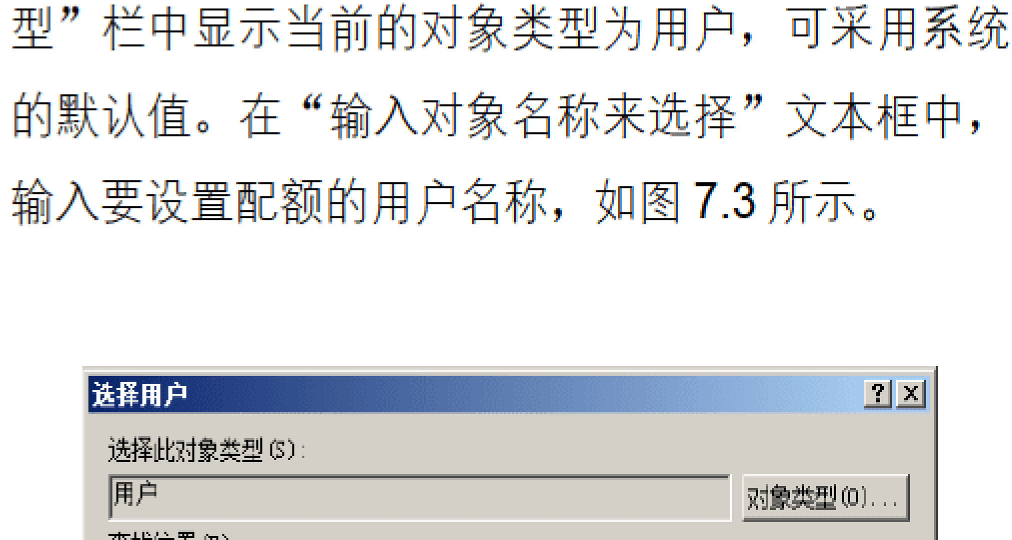
03 启用磁盘配额管理后，所有的用户都使用磁盘配额启动时设置的默认配额限制和配额警告级别。使用配额项目管理可以为每一个用户设置适合的磁盘配额，对用户的磁盘配额设置进行维护，并且可以记录每一个用户对磁盘空间的使用情况。

2. 为特定的用户制定磁盘配额

若让某一个用户使用更多的空间，可以为该用户单独制定更大的磁盘配额。

01 在“本地磁盘（D:）属性”对话框中，选择“配额”选项卡，单击“配额项”按钮，显示如图 7.2 所示“配额项”窗口。

02 选择“配额”下拉菜单中的“新建配额项”命令，显示“选择用户”对话框。在“选择此对象类型”栏中显示当前的对象类型为用户，可采用系统的默认值。在“输入对象名称来选择”文本框中，输入要设置配额的用户名称，如图 7.3 所示。



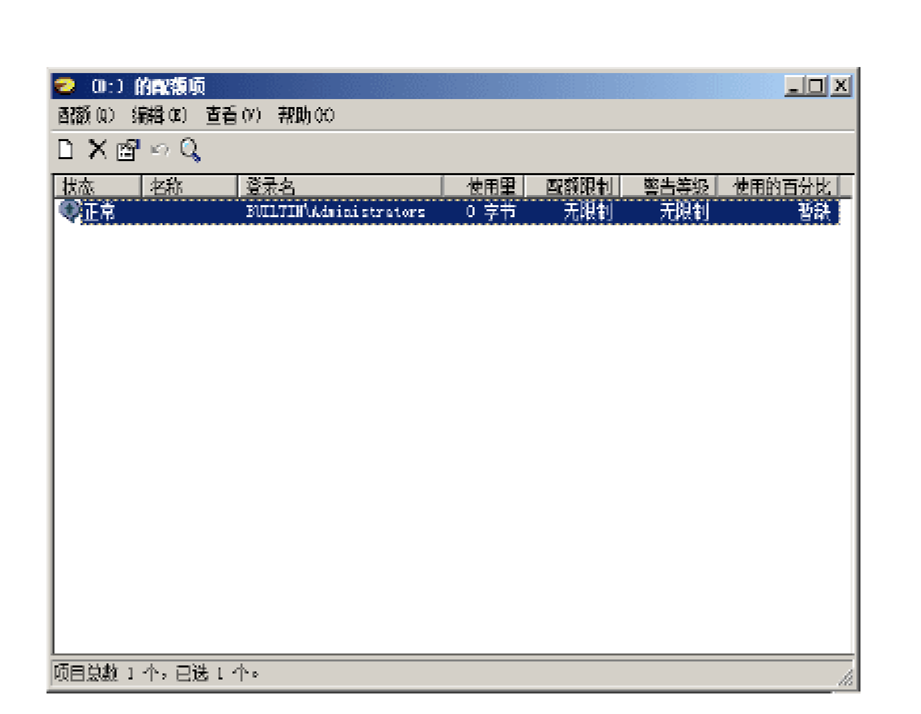


图 7.2　“（D:）的配额项”窗口

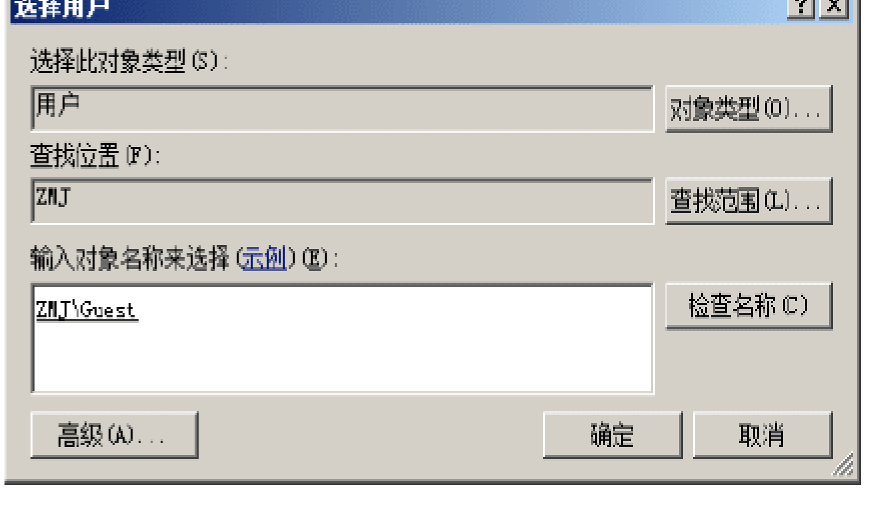


图 7.3　“选择用户”对话框

03 单击“确定”按钮，显示如图 7.4 所示“添加新配额项”对话框。选中“将磁盘空间限制为”单选按钮，并在其后文本框中为该用户设置访问磁盘的空间。

04 单击“确定”按钮，保存用户的磁盘配额设置，返回到“（D:）的配额项”窗口，可以看到新创建的用户“Guest”配额项显示在列表框中。



图 7.4　“添加新配额项”对话框

如果想删除指定用户的配额项，则可以右击用户名并选择快捷菜单中的“删除”选项。使用指定配额项具有以下优点：

- 登录到相同计算机的多个用户之间互不影响；
- 一个或多个用户不独占公用服务器上的磁盘空间；
- 在个人计算机的共享文件夹中，用户不使用过多的磁盘空间。

7.1.3 监控每个用户的磁盘配额使用情况

为用户设置好磁盘配额以后，除了可以借助“日志查看器”浏览磁盘占用情况外，在配额项窗口中，也可以监视每个用户的磁盘配额使用情况，并可单独设置每个用户可使用的磁盘空间。若想更改某用户的磁盘配额设置，可以在“配额项”窗口中双击该用户，显示如图 7.5 所示配额设置对话框，直接更改用户的磁盘空间限制及警告等级即可。

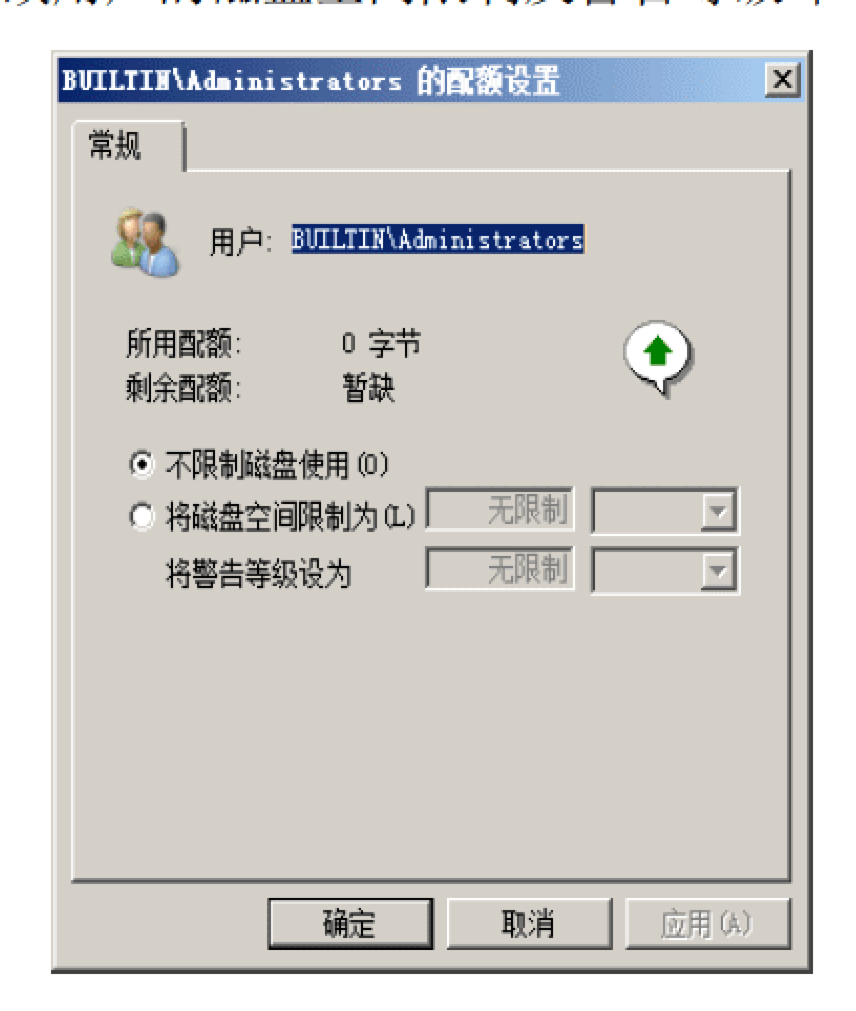


图 7.5 配额设置对话框

7.2 数据备份与恢复

无论怎样稳固的系统，都有可能遇到意外，都有可能崩溃，数据的备份与恢复便成了安全管理的重要课题。

7.2.1 Windows Server Backup

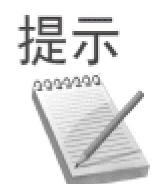
Windows Server Backup 是 Windows Server 2008 系统的新增功能之一，取代了原 Windows 系统中的备份工具（Ntbackup.exe）。Windows Server Backup 可以为用户的日常备份和恢复提供更为完整的方案和计划，既可以备份整个服务器（所有卷）的数据，也可以只备份用户选择的卷或状态信息，非常方便。

相对先前 Windows 系统中的备份和还原工具，Windows Server Backup 包括如下改进：

- 速度更快。Windows Server Backup 使用 VSS（Volume Shadow Copy Service，卷影复制服务）和增量备份技术，对系统数据和服务器数据进行备份。用户只需第一次创建一个完整的备份，接下来只需执行增量备份即可快速完成完整备份，所需时间更

少，效率更高；

- 操作简单。无论是数据库备份、还原还是制定备份计划，完全在向导指引下完成，操作更加简便。另外，用户还可以从备份中选择需要恢复的单个项目进行操作，而不必进行全面恢复，既节约时间又可以避免不必要的数据覆盖；
- 系统恢复更简单。Windows Server Backup 与新的 Windows 恢复工具配合使用，使操作系统恢复更加简单，而且还可以使用副本对其他类似硬件配置的服务器进行系统恢复(通常为未安装任何系统的全新计算机)；
- 恢复应用程序。Windows Server Backup 可以使用内置到应用程序中的 VSS 功能来保护应用程序数据；
- 非现场删除备份以便进行灾难保护。Windows Server Backup 可以将备份轮流保存到多个磁盘中，这样使管理员可以在非现场位置移动磁盘，将每个磁盘添加为一个计划备份的位置，如果第一个磁盘不在现场，则 Windows Server Backup 会自动将备份顺序保存到下一个磁盘中；
- 远程管理。Windows Server Backup 是基于 MMC 控制台的，管理员可以轻松连接至另一台远程计算机上，实现远程控制；
- 自动磁盘使用情况管理。在实施备份计划时，Windows Server Backup 会自动检查磁盘的使用情况，如果剩余空间不足，将自动重复使用陈旧备份的空间；
- 扩展命令行支持。Windows Server Backup 包含 Wbadmin 命令和文档，管理员可以在命令提示符窗口中执行备份和恢复任务；
- 支持可移动储介质。Windows Server Backup 允许管理员通过手动方式，将卷直接备份到光盘或其他可移动存储介质上。

提示  有关 Windows Server Backup 安装的介绍，请参考本书“第 4 章 活动目录安全”中的相关内容，此处不复赘述。

7.2.2　磁盘备份

“备份”并不难理解，主要用于不时之需。例如，开车出门会带备胎；长时间出差要给手机带备用电池等。数据备份，则是指在数据完好的情况下，对数据状态进行完整的拷贝。当数据丢失或损毁时，可以使用拷贝恢复到先前的完好状态。在 Windows Server 2008 系统中，管理员可以使用 Windows Server Backup 对磁盘数据进行备份。

01 在 Windows Server Backup 窗口中，单击“一次性备份”链接，显示如图 7.6 所示“一次性备份向导”对话框，依次单击“下一步”按钮，设置备份选项、配置和目标类型，在“备份选项”对话框中选中“不同选项”单选按钮。在“选择备份配置”对话框中，选中“整个服务器”单选按钮。在“指定目标类型”对话框中，选中“本地驱动器”单选按钮。

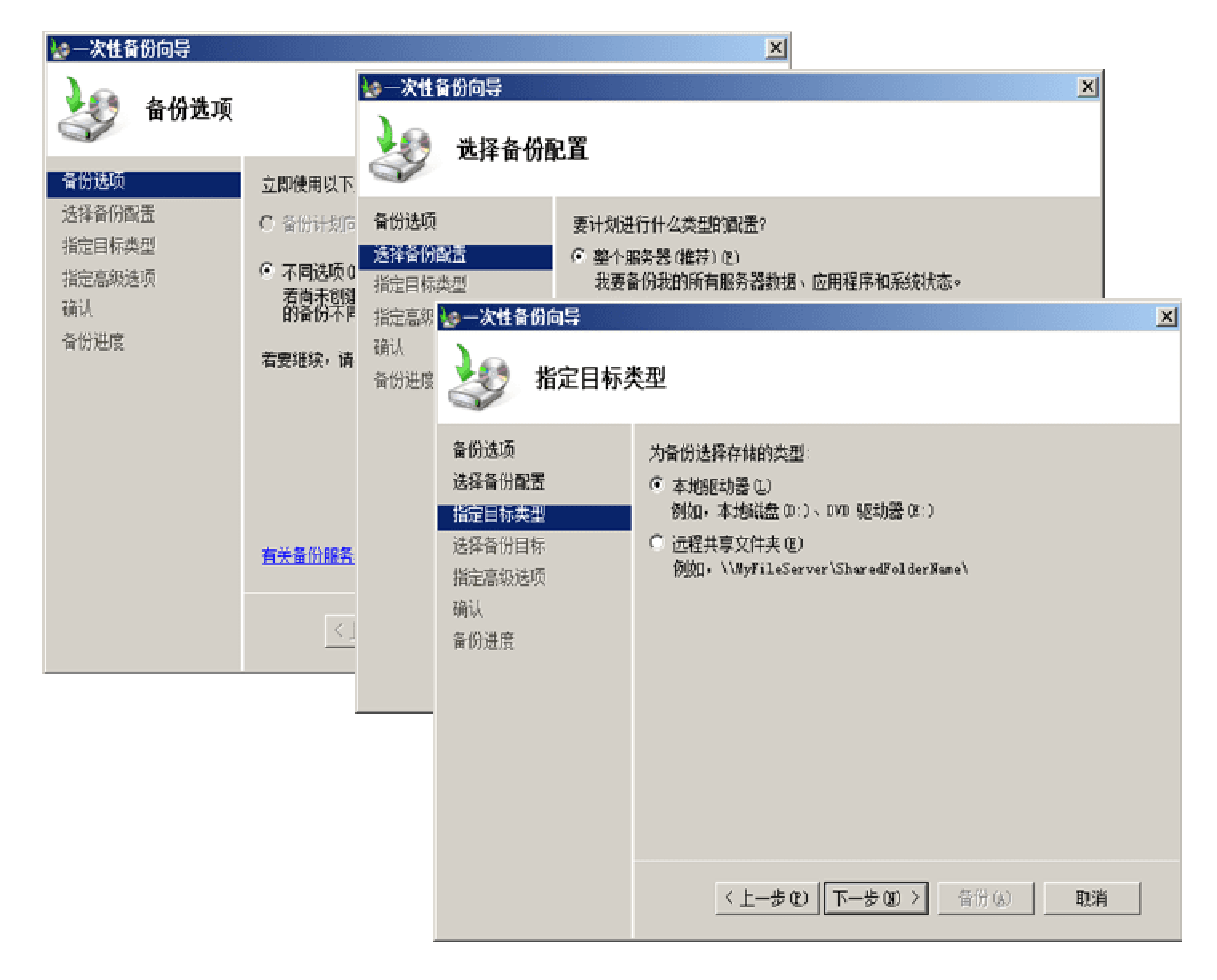


图 7.6　设置备份选项、配置和目标类型

02 依次单击“下一步”按钮，设置备份目标和其他高级选项，直至备份完成，如图 7.7 所示。在“选择备份目标”对话框中的“备份目标”下拉列表中，选择“本地磁盘（E:）”选项。“指定高级选项”对话框，选中“VSS 副本备份（推荐）”单选按钮。

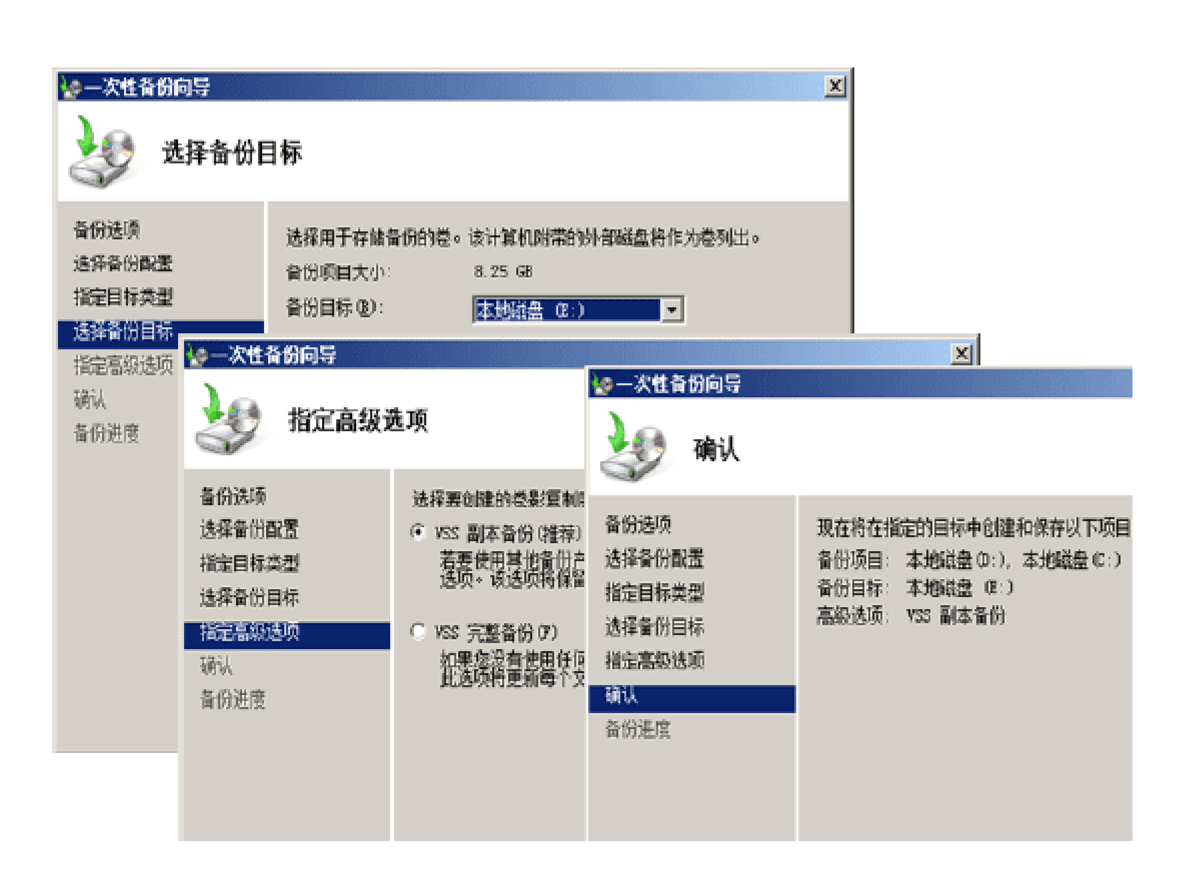


图 7.7　设置备份目标和高级选项

7.2.3　使用 Windows Server Backup 恢复磁盘数据

如果在数据完好状态下进行了磁盘备份，当出现磁盘故障或数据错误时，可以使用 Windows Server Backup 中的恢复向导，从备份中恢复磁盘数据。

01 选择“开始”→“管理工具”→“Windows Server Backup”命令，打开“Windows Server Backup”窗口。单击“操作”选项区域中的“恢复”链接，显示“恢复向导”对话框。提示选择要从哪个备份恢复服务器数据，既可以使用本地计算机中存储的备份，也可以使用远程计算机共享该服务器备份，这里

选择“此服务器”单选按钮。如果要从另一台服务器上的备份恢复服务器，则可以选择“另一个服务器”单选按钮。单击“下一步”按钮，在日期列表中选择备份的日期，如果同一天中保存了多个备份，则可以继续在“时间”下拉列表中选择不同的时间，如图 7.8 所示。

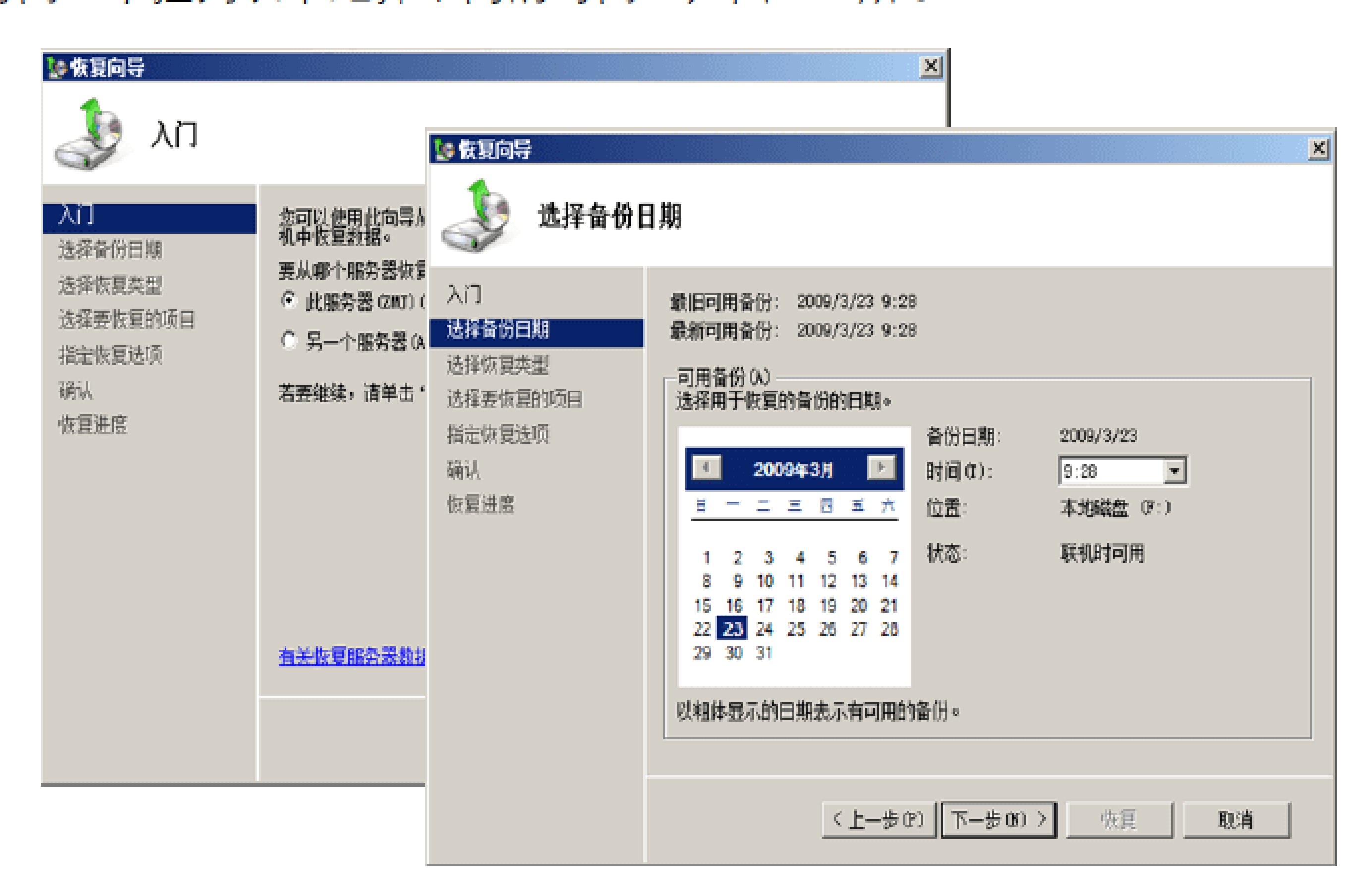


图 7.8　选择备份日期

02 依次单击“下一步”按钮，选择恢复类型和目标卷，在“选择恢复类型”对话框中，选择“文件和文件夹”单选按钮，可以根据需要选择要恢复的文件或文件夹中的数据，操作的前提是备份中包括文件和文件夹，应用程序恢复也是如此；选择“卷”单选按钮，则将恢复指定的磁盘分区。这里选择“卷”单选按钮，如图 7.9 所示，在“选择卷”对话框中选中备份中需要恢复的卷，在“目标卷”下拉列表中选择需要恢复到的卷。单击“下一步”按钮，提示恢复卷后将出现的问题。

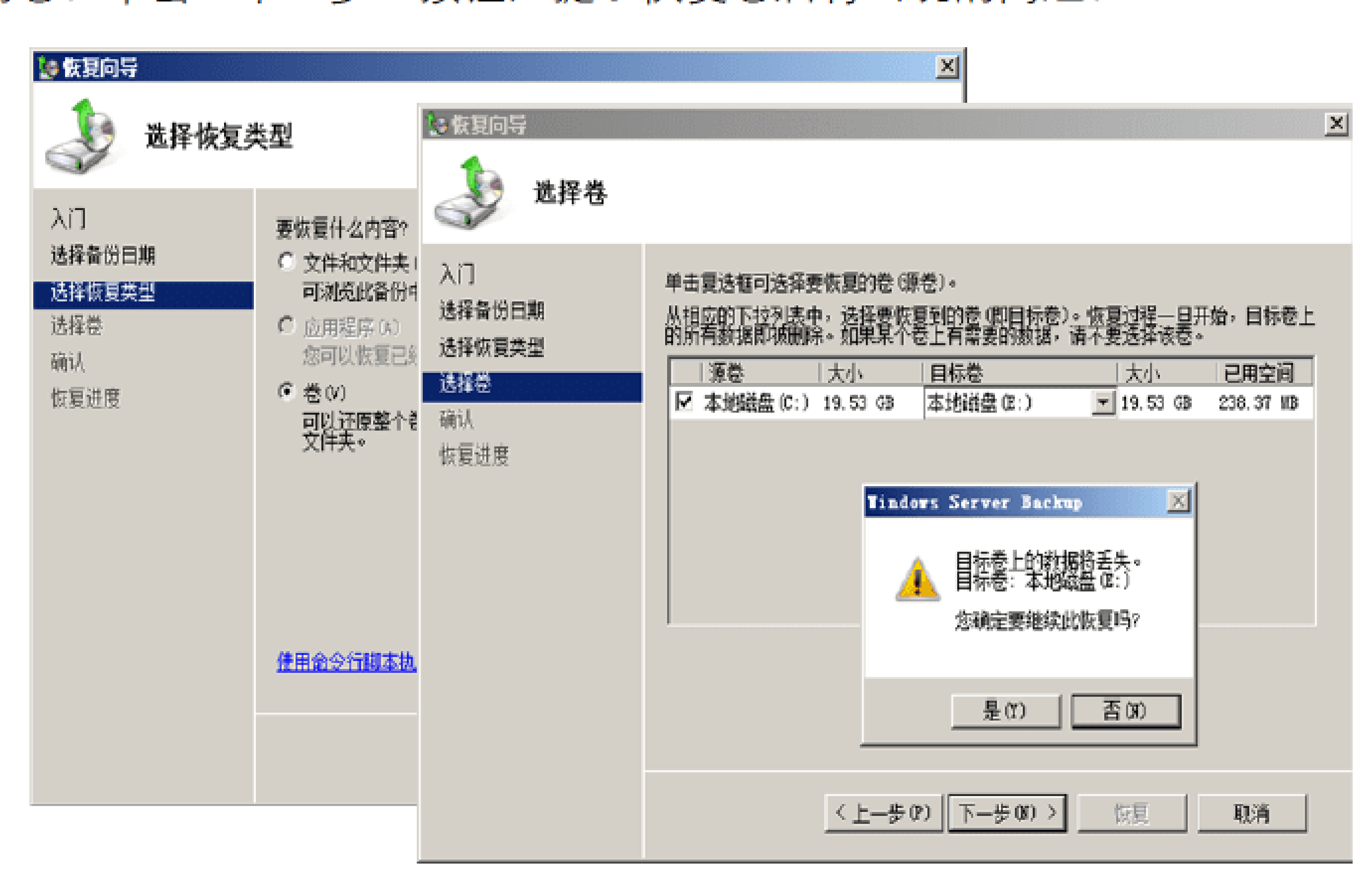


图 7.9　选择恢复类型和目标卷

03 单击“是”按钮，显示“确认”对话框。如果前面有漏选的需要恢复的项目，则可以单击“上一步”按钮返回修改。单击“恢复”按钮，即可开始恢复。根据恢复数据量的大小，所需的时间会有所不同，如果源数据位于远程计算机上，则恢复时间还取决于网络传输速度的限制，如图 7.10 所示。恢复完成后，单击“关闭”按钮，退出向导即可。

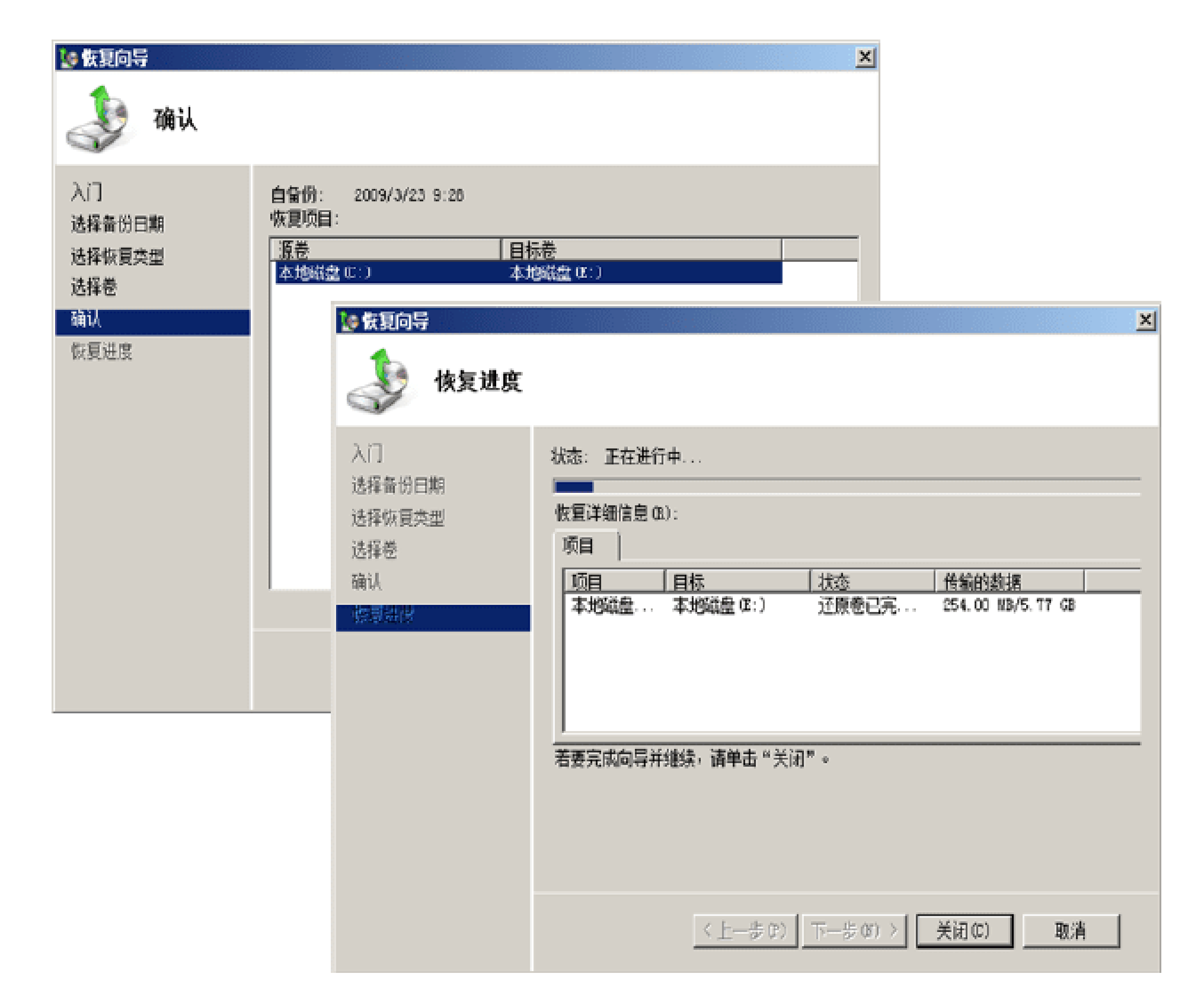


图 7.10 恢复数据

7.2.4 使用卷影副本实现磁盘数据恢复

在 Windows Server 2008 系统环境中，借助卷影副本功能可以为服务器中的共享文件夹创建即时点副本，一旦发生共享资源被用户误删除或误修改现象时，可以尝试访问对应时间点的共享文件夹副本，将特定时间点的共享内容恢复到误删除或误修改操作之前的状态。

1. 启动卷影副本

要让 Windows Server 2008 服务器系统中的共享文件夹“时光倒流”，首先需要针对该目标共享文件夹启用卷影副本功能。在进行这种操作时，必须先以特权账号登录到 Windows Server 2008 服务器系统桌面。

01 依次选择“开始”→“所有程序”→“附件”→“Windows 资源管理器”命令，在打开的窗口中找到保存目标共享文件夹的磁盘分区，右击该磁盘分区选项，在快捷菜单中选择“属性”选项，显示如图 7.11 所示“本地磁盘（D:）属性”对话框，切换至“卷影副本”选项卡。

02 选择要保存目标共享文件夹的磁盘卷，单击“启用”按钮，显示如图 7.12 所示“启用卷影复制”对话框，单击“是”按钮，完成设置后，Windows Server 2008 服务器系统就能自动按照默认设置启用目标共享文件夹的卷影拷贝功能。

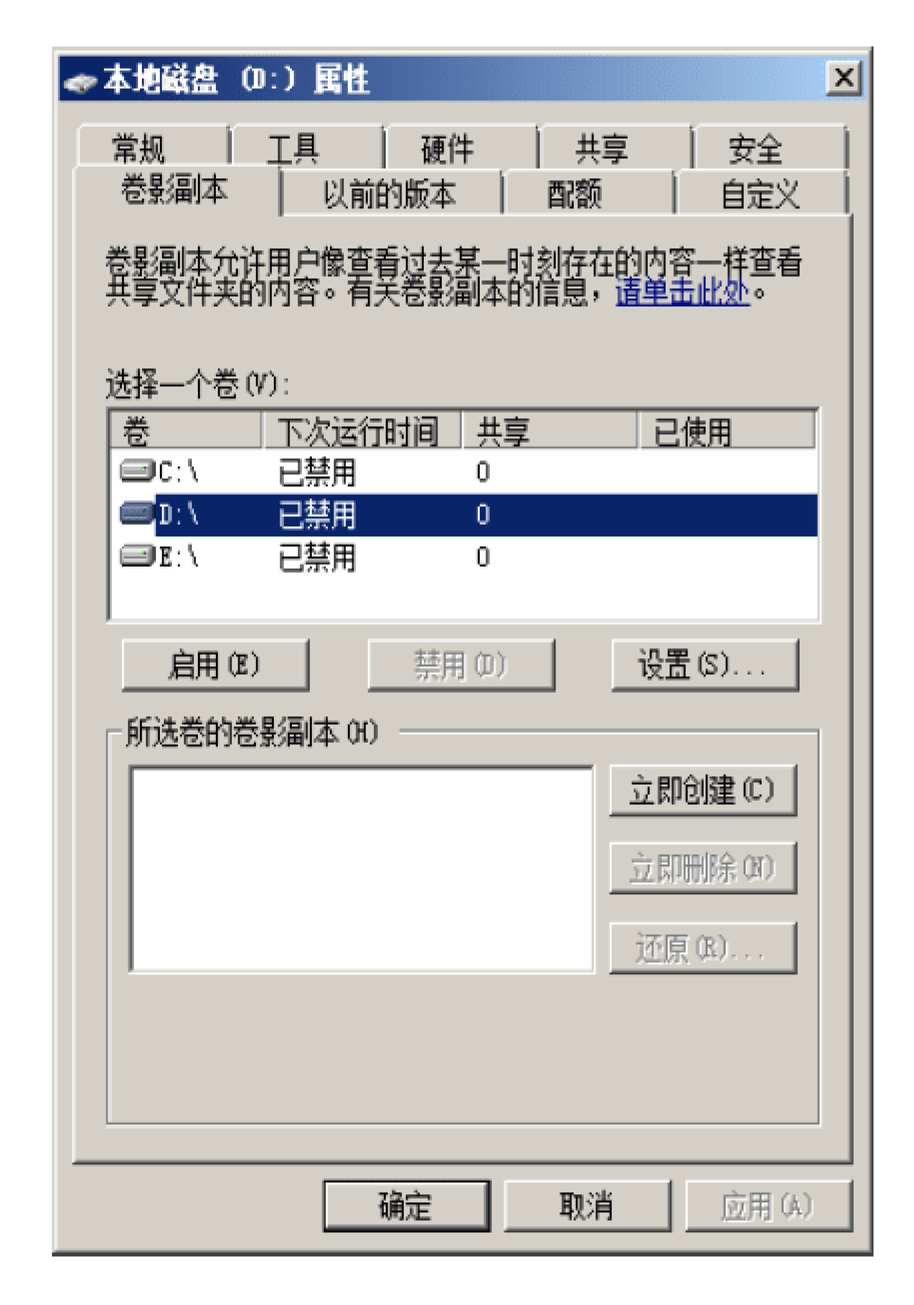


图 7.11　“本地磁盘（D:）属性”对话框

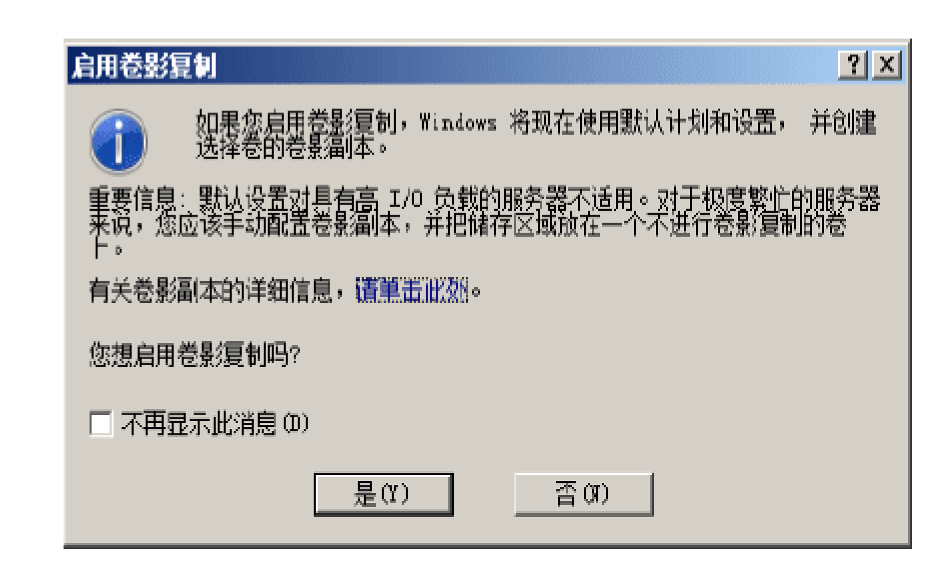


图 7.12　“启用卷影复制”对话框

2. 计划日程安排

打开“本地磁盘（D:）属性”对话框，单击“设置”按钮，显示“设置”对话框，在这里对运行计划参数、最大值参数、存储区域参数等进行有针对性设置。用户可以根据实际工作要求创建日程安排，单击“计划”按钮，显示如图 7.13 所示“日程安排”对话框。用户可以依照实际情况来定义创建即时点卷影副本的操作时间。最后单击“确定”按钮保存设置即可。

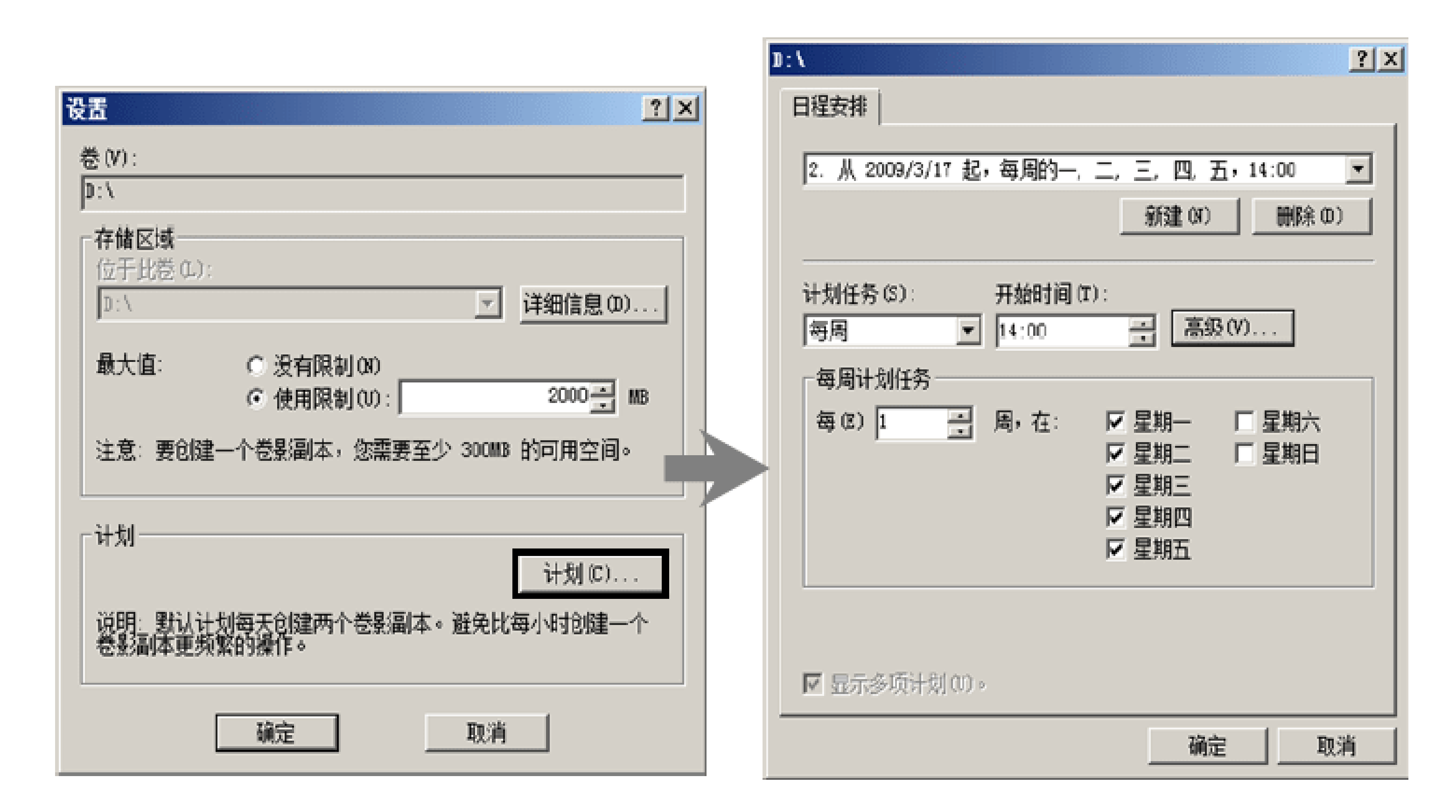
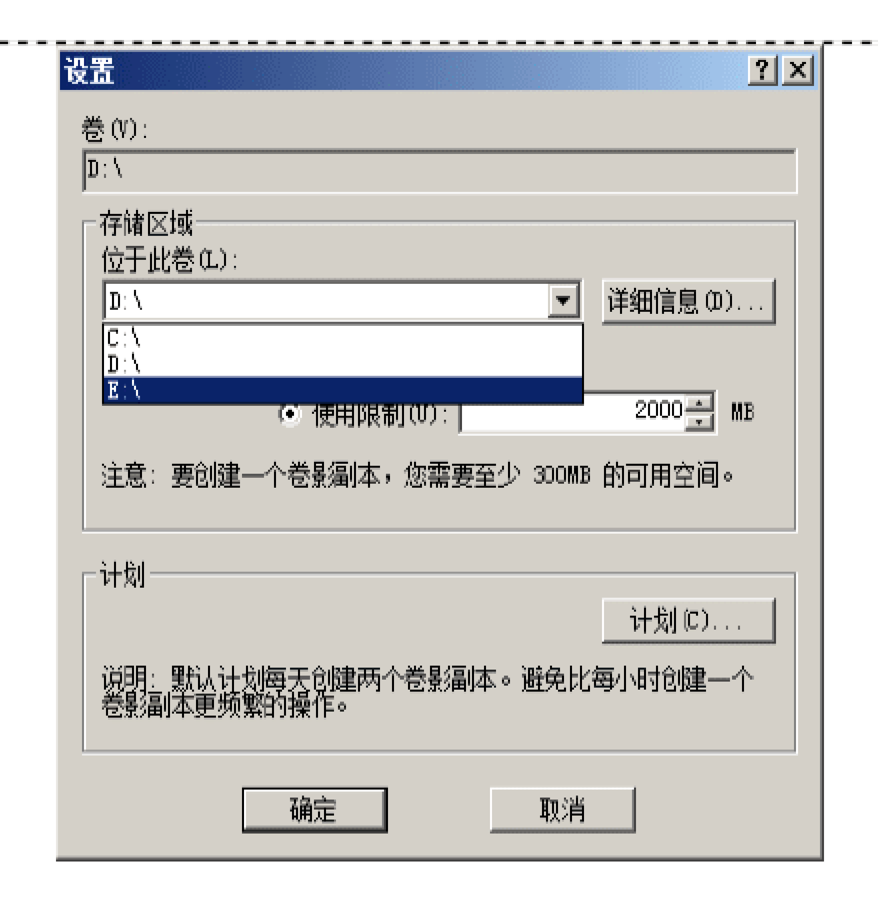


图 7.13　设置计划日程安排

3. 配置卷影副本

Windows Server 2008 服务器系统在缺省状态下会自动将即时点卷影副本保存在与目标共享资源相同的磁盘分区中，然而在同一个磁盘分区中，不利于连续保存多个即时点卷影副本，为此可以执行如下操作：



01 打开“本地磁盘（D:）属性”对话框，单击“设置”按钮，显示如图 7.14 所示“设置”对话框，在“存储区域”位置处，选择即时点卷影副本的存储位置，如“E:\”，通常应选择目标共享文件夹所在分区之外的其他磁盘分区。

02 单击“确定”按钮，即可完成卷影副本设置任务。

图 7.14 “设置”对话框



提示　只有在任何一个即时点卷影副本都还没有成功创建的时候，才可以对它的存储位置进行调整；如果已经有即时点卷影副本存在时，应该先将目标磁盘分区中的所有即时点卷影副本全部删除掉，才可以修改即时点卷影副本的存储位置。

完成卷影拷贝功能的启用、配置操作后，从局域网的普通工作站中打开服务器系统，右击目标共享文件夹，在弹出的快捷菜单中可以看到“还原以前的版本”选项，如图 7.15 所示。这就表示在对应的功能页面中，能够实现共享资源“时光倒流”的目的。

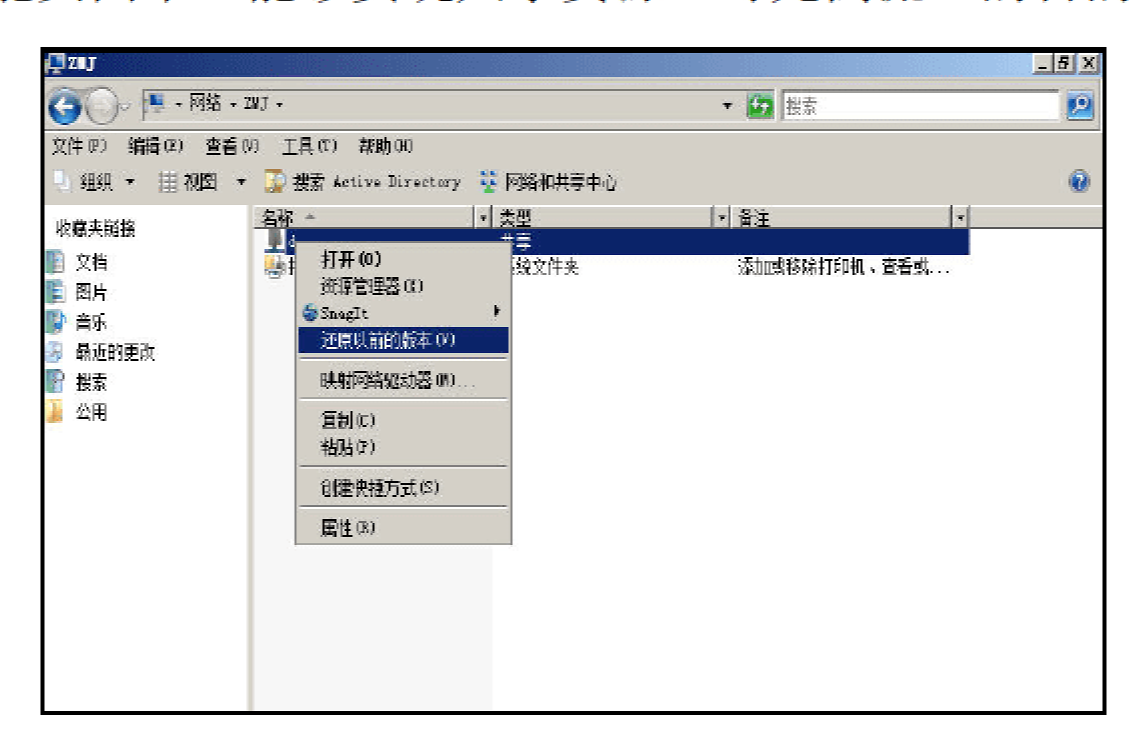


图 7.15 “还原以前的版本”选项

4. 管理副本

在 Windows Server 2008 服务器系统工作一段时间之后，或许已经在其中创建了很多个即时点卷影副本，为了便于以后可以快速找到误删除操作之前的那个即时点卷影副本，我们必须对服务器系统中的每一个即时点卷影副本进行合适的管理操作。

依次选择“开始”→“管理工具”→“服务器管理器”选项，打开“服务器管理器”窗口。在左侧窗口中依次选择“存储”→“磁盘管理”选项。右击“磁盘管理”选项，在弹出的快捷菜单中选择“所有任务”→“配置卷影副本”选项，显示如图 7.16 所示“卷影副本”对话框，可以在该设置窗口中依照实际情况将比较陈旧的即时点卷影副本删除掉，也可以重新创建一个新的即时点卷影副本，甚至还能将某个目标磁盘卷恢复到一个指定即时点卷影副本上。

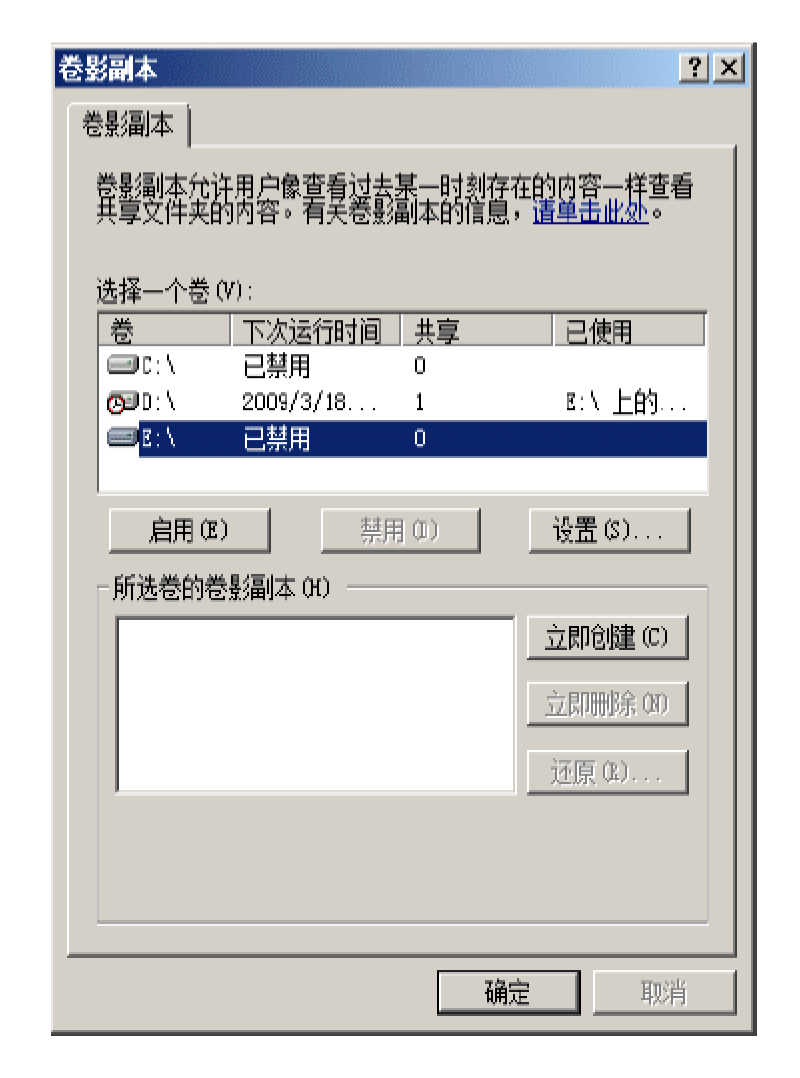


图 7.16　“卷影副本”对话框

7.3　软件 RAID

软件 RAID 是指包含在操作系统中，RAID 功能用软件方式由系统的核心磁盘代码来实现，完全基于操作系统。Windows Server 2003 和 Windows Server 2008 均可以实现软件 RAID，常用的 RAID 级别包括 RAID 0、RAID 1 及 RAID 5。软件 RAID 必须在多磁盘系统中才能实现。实现 RAID 1 最少要拥有 2 块硬盘，实现 RAID 5 最少要拥有 3 块硬盘。通常情况下，操作系统所在磁盘采用 RAID 1，而数据所在磁盘采用 RAID 5。

7.3.1　初步认识磁盘

想要正确理解和执行磁盘管理功能，先要从一些基本却很重要的专业术语开始，其中包括实现软件 RAID 所需的磁盘类型、文件格式以及磁盘管理方式等。

1. 基本磁盘

基本磁盘是指允许操作系统直接访问的物理磁盘。基本磁盘可包含 4 个主磁盘分区，或 3 个主磁盘分区加 1 个具有多个驱动器的扩展磁盘分区。如果要创建跨越多个磁盘的分区，必须先利用“磁盘管理”或 Diskpart.exe 命令行工具将基本磁盘转换为动态磁盘。

2. 动态磁盘

动态磁盘是提供基本磁盘不能提供的功能的物理磁盘，例如对跨多个磁盘的卷的支持。动态磁盘使用一个隐藏的数据库来跟踪有关本磁盘和计算机中其他动态磁盘上的动态卷的信息。可以使用“磁盘管理”控制台或 Diskpart.exe 命令行工具将基本磁盘转换为动态磁盘。如果将一个基本磁盘转换为动态磁盘，所有现有基本卷都将变为动态卷。

3. 分区

分区是基本磁盘类型中的术语，它是能像物理上独立磁盘那样工作的物理磁盘部分。创建

分区后，将数据存储在该分区之前必须将其格式化并指派驱动器号。在基本磁盘上，分区被称为基本卷，它包含主要分区和逻辑驱动器。在动态磁盘上，分区称为动态卷，它包含简单卷、带区卷、镜像卷和 RAID 5 卷。

4. 卷

卷通常是动态磁盘类型中的术语，与基本磁盘中的分区类似，也是硬盘上的存储区域。使用一种文件系统可以格式化卷，并给卷指派一个驱动器号。单击“Windows 资源管理器”或“计算机”中某个卷的图标可以查看该卷的内容。一个硬盘可以有多个卷，一个卷可以跨越多个磁盘。

5. 基本卷

基本卷是驻留在基本磁盘上的主磁盘分区或逻辑驱动器。

6. 动态卷

动态卷是驻留在动态磁盘上的卷。Windows 系统支持 5 种类型的动态卷：简单卷、跨区卷、带区卷、镜像卷和 RAID 5 卷。动态卷通过使用文件系统来格式化，并有一个分配给它的驱动器号。

7. 主启动记录（MBR）

主启动记录是硬盘上的第一个扇区，启动计算机的过程就是从这里开始的。MBR 包含磁盘的分区表和称作“主引导代码”的少量可执行代码。

8. 主磁盘分区

主磁盘分区是在基本磁盘上创建的一种分区类型。主磁盘分区是物理磁盘的一部分，它像物理上独立磁盘那样工作。对于基本主启动记录磁盘，在一个基本磁盘上最多可以创建 4 个主磁盘分区，或者 3 个主磁盘分区和 1 个有多个逻辑驱动器的扩展磁盘分区。对于 GUID 分区表磁盘，最多可创建 128 个主磁盘分区，也称为“卷”。

9. 扩展磁盘分区

扩展磁盘分区是一种分区类型，只可以在基本的主启动记录磁盘上创建。如果想在基本的 MBR 磁盘上创建 4 个以上的卷，扩展磁盘分区将非常有用。与主磁盘分区不同的是，不需要用文件系统格式化扩展磁盘分区，然后给它指派一个驱动器号。相反，可以在扩展磁盘分区中创建一个或多个逻辑驱动器。创建逻辑驱动器之后，再将其格式化并为其指派一个驱动器号。一个 MBR 磁盘可以包含最多 4 个主磁盘分区，或 3 个主磁盘分区、1 个扩展磁盘分区和多个逻辑驱动器。

10. 系统分区

系统分区是包含加载 Windows 系统所需的硬件特定文件的分区。系统分区可以与启动分区相同，如启动分区都是磁盘的第一个分区，分区符号为“C”，而安装 Windows 系统时可以安装在任何分区或逻辑驱动器上，如通常所说的“D”、“E”盘。

7.3.2　准备动态磁盘

RAID 对磁盘要求比较严格，必须选用相同品牌、型号和容量的磁盘来组建 RAID。同时，组建 RAID 之前必须先将基本磁盘转换为动态磁盘。

01 依次选择“开始”→“管理工具”→“计算机管理”→“存储”→“磁盘管理”命令，显示计算机中安装的所有磁盘。右击要设置为动态磁盘的硬盘，在快捷菜单中选择“转换到动态磁盘”命令，显示如图 7.17 所示“转换为动态磁盘”对话框。

02 单击“确定”按钮，显示如图 7.18 所示“要转换的磁盘”对话框，要求用户对要升级为动态磁盘的硬盘进行确认。因为该操作是不可逆的，即基本磁盘可以升级为动态磁盘，但动态磁盘却不能降级为基本磁盘。



图 7.17　选择需要转换为动态磁盘的基本磁盘

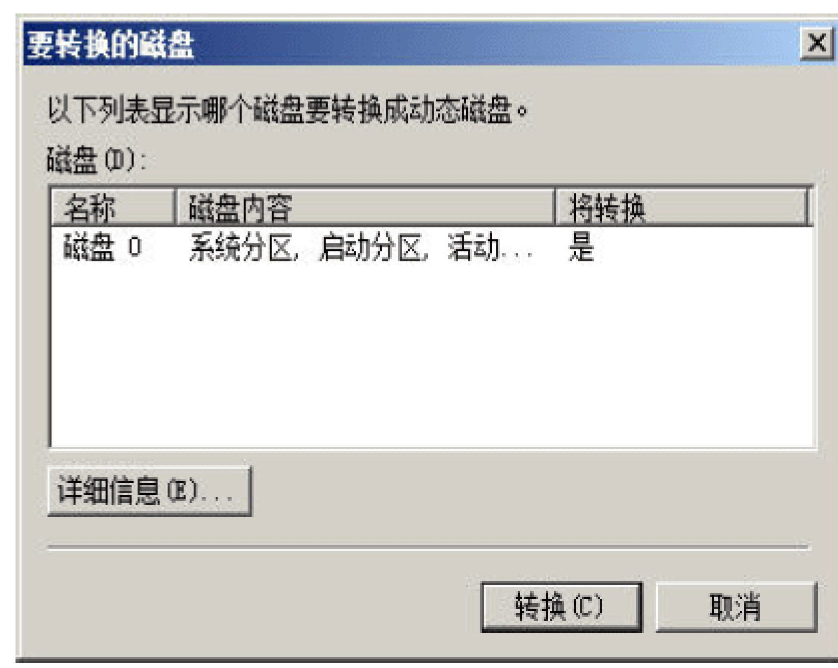


图 7.18“要转换的磁盘”对话框

03 单击“转换”按钮，显示如图 7.19 所示“磁盘管理”对话框，系统再次要求用户对磁盘升级予以确认。当将该磁盘升级为动态磁盘后，其他操作系统将不能再从该磁盘启动。

04 单击“是”按钮，系统开始升级过程。转换完成后，如图 7.20 所示。

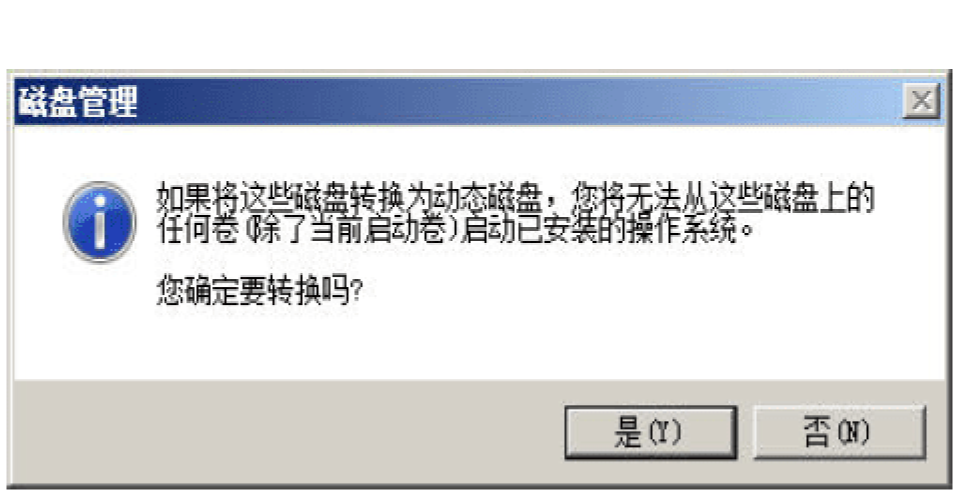
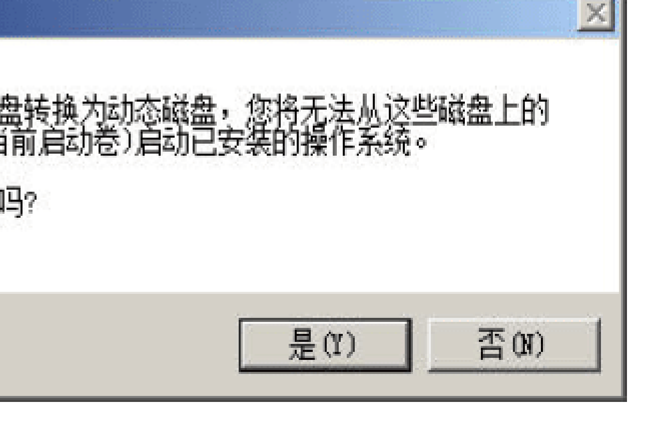



图 7.19　“磁盘管理”提示框

图 7.20　转换磁盘

需要注意的是，在转换到动态磁盘时，应当注意以下几个方面的问题：

- 必须以管理员或管理组成员的身份登录才能完成该过程。如果计算机与网络连接，则网络策略设置也可能阻止完成此步骤；
- 将基本磁盘转换到动态磁盘后，不能将动态卷改回到分区。相反，必须删除磁盘上的所

有动态卷，然后使用“还原为基本磁盘”命令；

- 在转换磁盘之前，关闭在那些磁盘上运行的程序；
- 为保证升级成功，任何要升级的磁盘都必须至少包含 1MB 的未分配空间。在磁盘上创建分区或卷时，“磁盘管理”将自动保留这个空间，但是带有其他操作系统创建的分区或卷的磁盘上可能没有这个空间；
- 扇区大小超过 512 字节的磁盘，不能从基本磁盘升级为动态磁盘；
- 一旦转换，动态磁盘就不能包含分区或逻辑驱动器。

7.3.3 实现软 RAID

软 RAID 也必须在多磁盘系统中才能实现。实现 RAID-1 最少要拥有 2 块硬盘，实现 RAID-5 最少要拥有三块硬盘。通常情况下，操作系统所在磁盘采用 RAID-1，而数据所在磁盘采用 RAID-5。由于各种卷的创建方式基本相同，这里以 RAID-5 卷为例进行介绍。

1. 实现 RAID-5

创建或修复镜像卷或 RAID-5 卷时，需要使用型号、大小和制造商都相同的磁盘。这可以确保磁盘相同，而且简化了创建新的镜像卷或 RAID-5 卷以及替换出现故障磁盘的过程。另外，还建议具有可用的备用磁盘和磁盘控制器，这样，当磁盘或磁盘控制器出现故障时，可快速使用同一类型的磁盘或磁盘控制器替换出现故障磁盘或磁盘控制器。

01 右击要设置软 RAID 的硬盘，在快捷菜单中选择“新建 RAID-5 卷”命令，启动“新建 RAID-5 卷”向导。单击“下一步”按钮，显示如图 7.21 所示“选择磁盘”对话框。在左侧“可用”列表框中，选择要添加的磁盘，单击“添加”按钮，即可将其添加至该 RAID-5 卷，并显示在“已选的”列表框中。在“选择空间量”文本框中，输入新建卷的大小。

02 单击“下一步”按钮，显示如图 7.22 所示“分配驱动器号和路径”对话框。选中“分配以下驱动器号”单选按钮，并在其下拉列表中指派一个该 RAID-5 卷的驱动器号。

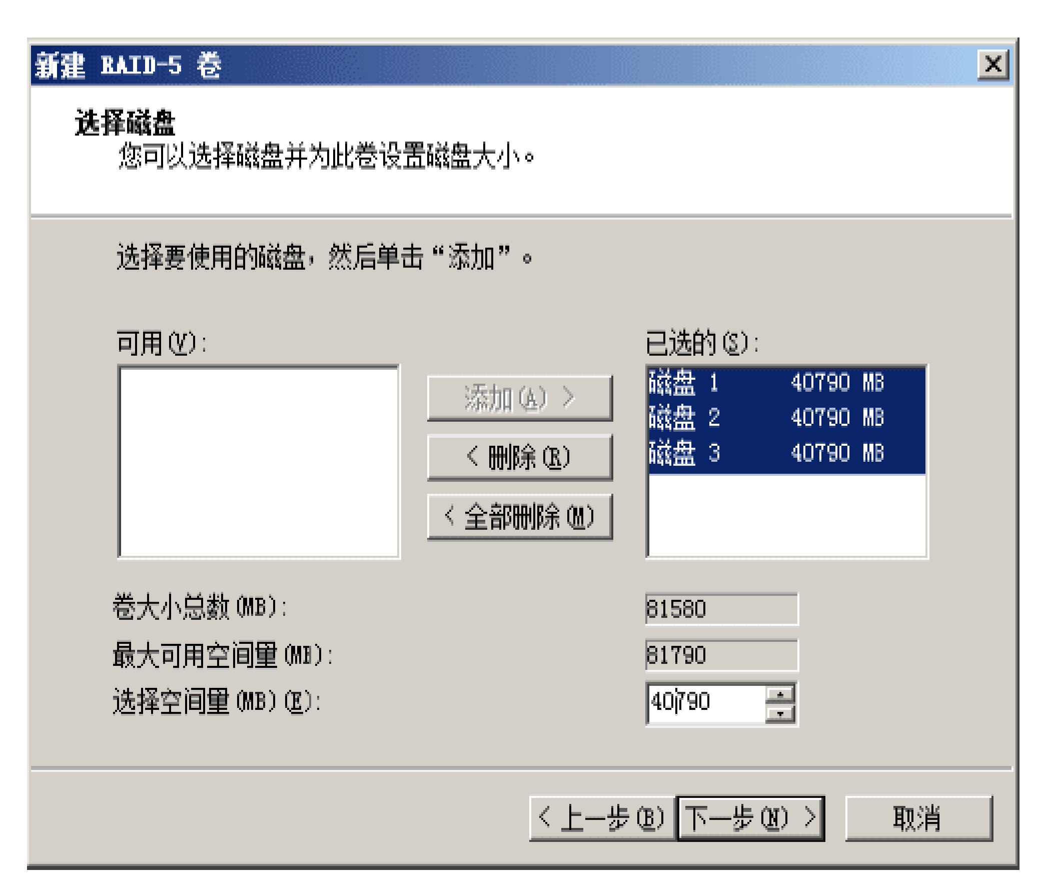


图 7.21 “选择磁盘”对话框



图 7.22 “分配驱动器号和路径”对话框



03 单击“下一步”按钮，显示如图 7.23 所示“卷区格式化”对话框。选择“按下列设置格式化这个卷”选项，并采用默认的 NTFS 文件系统和分配单位大小。在“卷标”文本框中，输入该 RAID-5 卷的卷标。如果选中“执行快速格式化”复选框，可以在创建完成后，快速格式化该卷。

04 单击“下一步”按钮，显示“正在完成新建 RAID-5 卷向导”对话框，新卷创建完成。单击“完成”按钮，系统自动格式化新创建的卷。至此，RAID-5 卷创建完成，如图 7.24 所示。

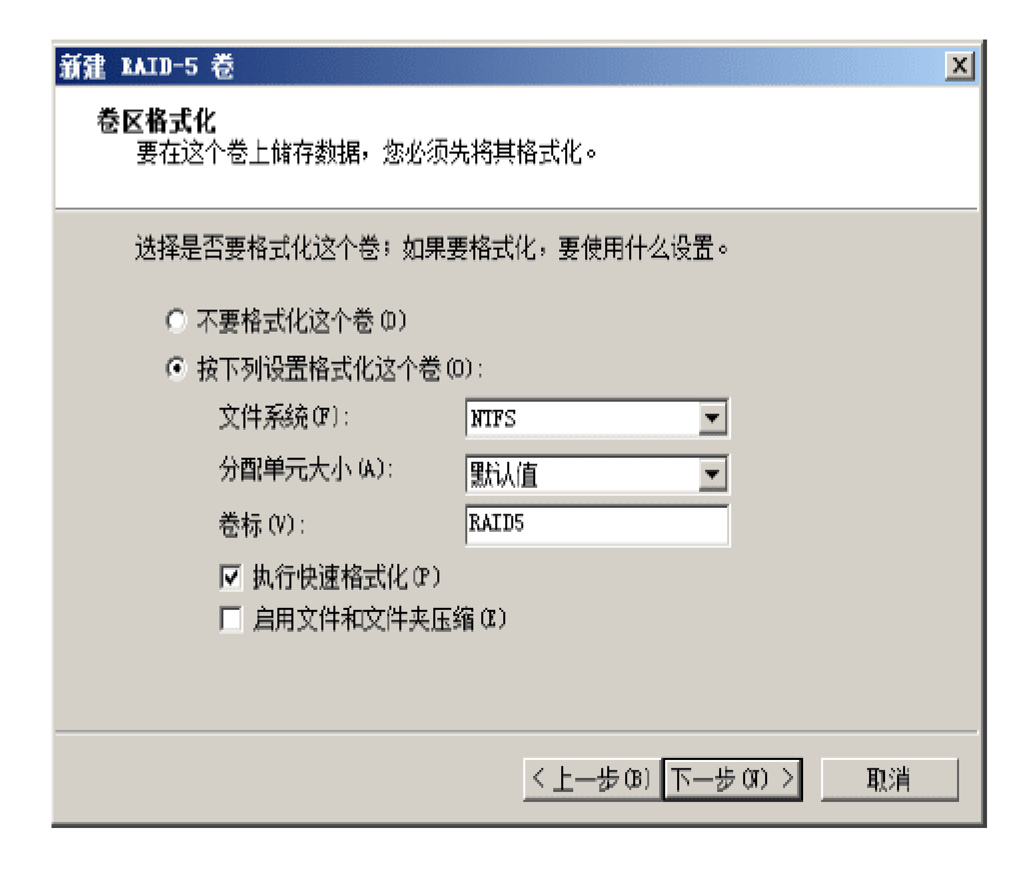


图 7.23　“卷区格式化”对话框



图 7.24　RAID-5 卷创建完成

2. 添加镜像卷

对于已有的动态磁盘，可以简单地通过添加镜像卷的方式提高数据的安全性。例如在安装操作系统时，计算机上只安装了一块磁盘，此时为保证系统安全，可以为系统磁盘添加镜像卷。

01 在“磁盘管理”中，右击要添加镜像磁盘的动态磁盘，在快捷菜单中选择“添加镜像”选项，显示如图 7.25 所示“添加镜像”对话框，在磁盘列表中选择要设置为镜像的动态磁盘。

02 单击“添加镜像”按钮，镜像添加完成，如图 7.26 所示。需要注意的是，添加为镜像的磁盘空间必须大于或等于现存卷。

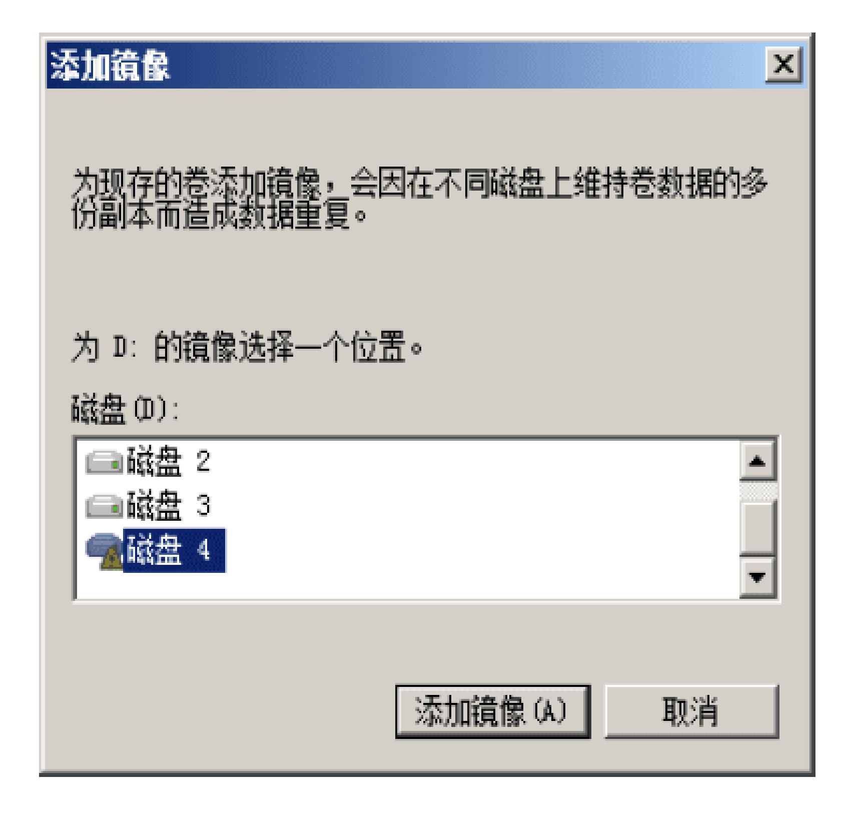


图 7.25　“添加镜像”对话框

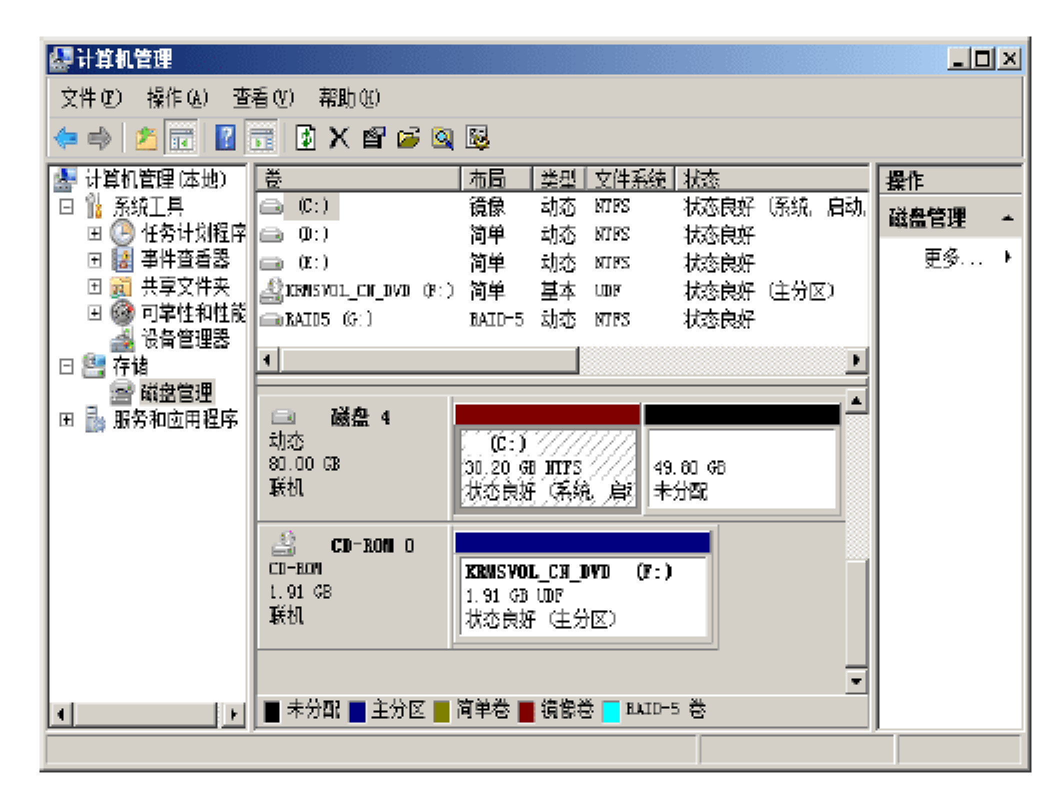


图 7.26　镜像添加完成

镜像添加完成后，系统将自动开始磁盘间的同步操作，这可能会需要较长时间。

小　　结

磁盘安全是系统安全中最重要的环节之一，作为一名网络管理员既要确保网络用户能够正常使用所需的文件，又要防止其滥用，以确保文件的安全性。通常情况下，可以通过为文件设置适当的访问权限，限制用户的非法访问，达到访问控制的目的。在 Windows Server 2008 系统中，还增加了各种新的技术手段，进一步确保了系统的安全性。

习　　题

1. Windows Server 2008 的系统分区必须为哪种分区格式的文件系统？
2. Windows Server 2008 中共享权限可以分为哪三种？
3. Windows Server 2008 系统中新增了哪个功能取代了原 Windows 系统中附带的备份功能（Ntbackup.exe）？
4. Windows Server 2008 系统中文件服务器可以利用什么工具实现磁盘阵列？

实验：恢复磁盘数据

实验目的

掌握如何利用 Windows Server Backup 恢复磁盘数据。

实验内容

使用 Windows Server Backup 中的恢复向导从备份恢复磁盘数据。

实验步骤

1. 打开 Windows Server Backup。
2. 设置恢复操作。
3. 选择备份日期。
4. 选择恢复类型。
5. 选择需要恢复的卷。
6. 完成恢复。

第 8 章

文件访问安全

文件安全是系统安全中最重要的课题之一，既要确保网络用户能够正常使用所需的文件，又要防止其滥用，确保文件的安全性。通常情况下，可以通过为文件设置适当的访问权限，限制用户的非法访问，达到访问控制的目的。另外，在 Windows Server 2008 系统中，还提供了 AD RMS 文件安全保护功能，可以确保局域网内文件的安全访问。

本章导读

- NTFS 访问权限安全
- 文件夹共享安全
- 共享文件夹的管理
- 权限管理服务
- 文件数据备份
- 文件数据恢复

8.1　NTFS 访问权限安全

NTFS 是网络服务器上使用最多的文件系统，其主要特点是安全性高，允许管理员为文件配置详细的访问控制权限。Windows Server 2008 要求，系统分区必须为 NTFS 文件系统，便于为各种网络服务数据及日志信息，提供更安全的存储和访问环境。

8.1.1　NTFS 基本认识

NTFS 即 NT File System，是 Windows XP 和 Windows Server 2003 推荐使用的文件系统，是 Windows Vista 和 Windows Server 2008 必须的文件系统。NTFS 文件系统的核心结构叫作主文件表（Master File Table）。NTFS 会对主文件表的关键部分做出数份拷贝，以防止数据的残缺或丢失。

与其他现有文件系统相比，NTFS 文件系统可以为文件存储提供更高的安全性和可靠性。例如，NTFS 通过使用标准的事务处理记录和还原技术来保证卷的一致性。如果系统出现故障，NTFS 将使用日志文件和检查点信息来恢复文件系统的一致性。另外，NTFS 还可以提供诸如文件和文件夹权限、加密、磁盘配额和压缩这样的高级功能。

NTFS 文件系统具有以下功能和优点：

- 更好的伸缩性使扩展为大驱动器成为可能。NTFS 的最大分区或卷比 FAT 的最大分区或卷大得多，当卷或分区大小增加时，NTFS 的性能并不会降低，而在此情形下 FAT 的性能会降低；
- Active Directory。通过 Active Directory 可容易地查看和控制网络资源。使用域可以在保持管理简单的情况下微调安全选项。域控制器和 Active Directory 需要使用 NTFS；
- 压缩功能，包括压缩或解压缩驱动器、文件夹或者特定文件的功能，但是不可以同时压缩和加密某个文件；
- 文件加密，它极大地增强了安全性，但是不可以同时压缩和加密某个文件；
- 可以对单个文件而不仅仅对文件夹设置权限；
- 远程存储，通过使可移动媒体（如磁带）更易访问，从而扩展了磁盘空间。恢复磁盘活动的日志记录，它允许 NTFS 在断电或发生其他系统问题时尽快地恢复信息；
- 稀疏文件。稀疏文件是一些大型文件，应用程序以一种仅需有限磁盘空间的方式创建了这些文件。也就是说，NTFS 只为文件的写入部分分配了磁盘空间；
- 磁盘配额，可用来监视和控制单个用户使用的磁盘空间量。

8.1.2　NTFS 文件夹权限和 NTFS 文件权限

对于 NTFS 分区上的文件和文件夹，管理员可以通过 NTFS 权限限制不同用户帐户的访问权限。文件和文件夹的 NTFS 权限有两种类型：显式权限和继承权限。其中，显式权限是系统创建对象时，默认赋予用户帐户的访问和操作权限；继承权限是从父对象传播到当前对象的权限。继承权限可以减轻管理权限的任务，并确保给定容器器内所有对象之间的权限一致性。默认情况下，文件将自动继承来自其父文件夹的 NTFS 权限设置。

1. NTFS 文件夹权限

NTFS 文件夹权限及允许用户完成的操作如表 8.1 所示。

表 8.1　NTFS 文件夹权限

NTFS 文件夹权限	允许用户完成的操作
读取	查看该文件夹中的文件和子文件夹； 查看文件夹的所有者、权限和属性（如只读、隐藏、存档和系统）
写入	在该文件夹内新建文件和子文件夹； 更改文件夹属性，查看文件夹的所有者和权限
列出文件夹目录	查看该文件夹中的文件和子文件夹的名称
读取及运行	完成“读取”权限和“列文件夹目录”权限所允许的操作； 漫游各个文件夹，以便访问其他文件和文件夹，即使该用户没有那些文件夹的权限
修改	完成“写入”权限及“读取及执行”权限所允许的操作； 删除文件夹
完全控制	完成其他所有 NTFS 权限允许的操作； 更改权限，取得所有权和删除子文件夹和文件

2. NTFS 文件权限

NTFS 文件权限及允许用户完成的操作如表 8.2 所示。

表 8.2　NTFS 文件权限及允许用户完成的操作

NTFS 文件权限	允许用户完成的操作
读取	读该文件和查看文件属性、所有者及权限
写入	覆盖该文件，更改文件属性和查看文件的所有者和权限
读取及运行	完成“读取”权限所允许的操作； 运行应用程序
修改	完成“写入”权限和“读取及运行”权限所允许的操作； 修改和删除文件
完全控制	完成其他所有 NTFS 文件权限所允许的操作； 更改权限和取得所有权。

8.1.3　多重 NTFS 权限

管理员可以根据需要为 NTFS 分区上的文件和文件夹同时设置 NTFS 权限，而文件夹和文件有可能是包含与被包含的关系，所以必然会产生资源权限的重复，从而直接导致文件夹或文件最终的 NTFS 权限并非是管理员真正需要的结果。

1. 权限是累积的

用户对一个资源的最终权限，是为该用户指定的全部 NTFS 权限和为该用户所属组指定的全部 NTFS 权限之和。如果某用户拥有一个文件夹的读取权限，同时又是对该文件夹有写入权限用户组的成员，则最终该用户对这个文件夹既有读取权限，也有写入权限。

例如，用户帐户 liuxh 隶属于 Manager 组，并且该用户本身对 Folder 文件夹具有读取权限，而其所在用户组 Manager 对 Folder 文件夹拥有写入权限，所以最终用户 liuxh 对 Folder 文件夹的有效权限就是“读取+写入”，如图 8.1 所示。

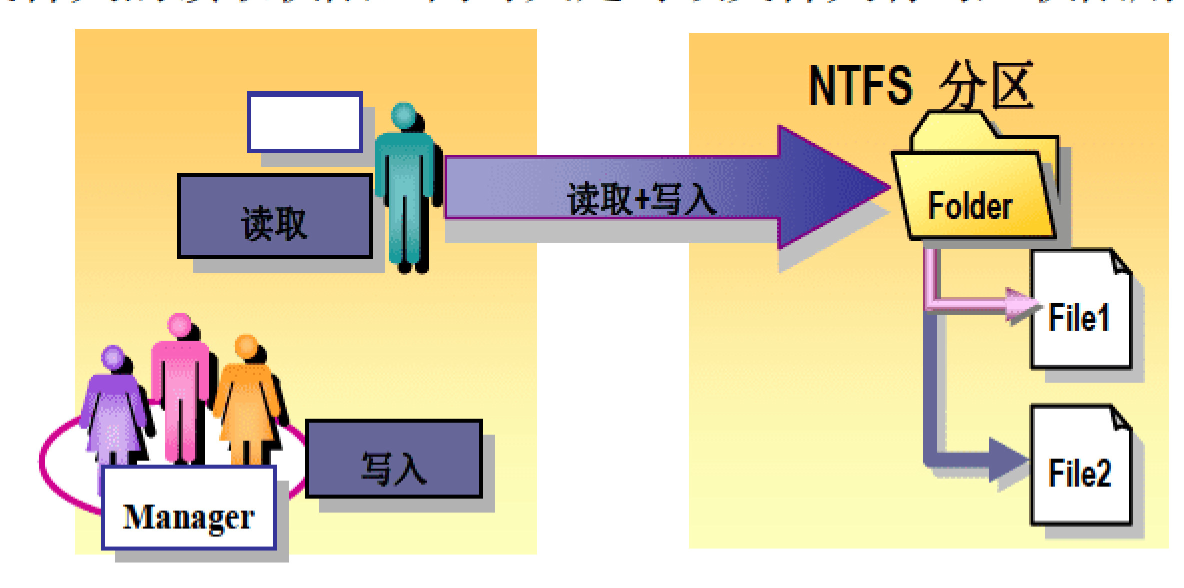


图 8.1　权限是累积的

2. 文件权限优先于文件夹权限

NTFS 文件权限优先于 NTFS 文件夹权限，即用户只要有访问一个文件的权限，即使没有访问该文件所在文件夹的权限，也可以访问该文件。用户可以通过通用命令规则（UNC）或本地路径，从各自的应用程序打开有权访问的文件。即使该用户由于没有包含该文件夹的权限而看不到该文件夹，但仍然可以访问那些文件。例如，Folder 文件夹下包含 Files1 和 Files2 两个文件，Folder 的文件夹权限允许用户 liuxh 写入，但 File2 的 NTFS 权限只允许用户 liuxh 读取，此时用户 liuxh 的有效权限就是对 Folder 文件夹（包括 File1）的写入权限和对 File2 的读取权限，如图 8.2 所示。

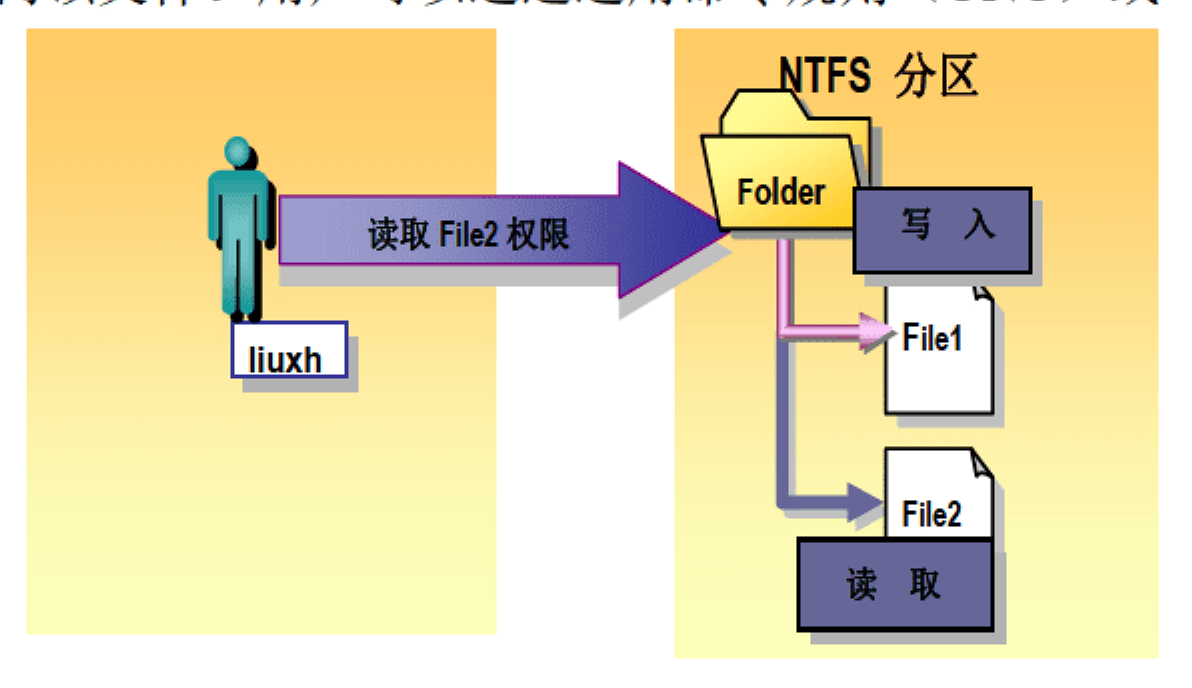


图 8.2　文件权限优先于文件夹权限

3. 拒绝权限优先于其他权限

在 Windows 系统所有 NTFS 权限中，拒绝权限优先于其他任何权限。即使用户作为一个组的成员有权访问文件或文件夹，一旦该用户被设置了拒绝访问权限，则最终将剥夺该用户可能拥有的任何其他权限。在实际使用中，应当尽量避免使用拒绝权限，因为允许用户和组进行某种访问，要比设置拒绝权限更容易做到。而事实上，只需巧妙地构造组和灵活组织文件夹中的资源，即可通过各种各样的“允许”权限满足访问控制的需求。

例如，User1 同时属于 Group B 组和 Group A 组。其中，User1 拥有对 Folder A 的读取权限，Group B 拥有对 Folder A 的读取和写入权限，Group A 则被禁止对 File2 的写入操作。因此，User1 拥有对 Folder A 和 File1 的读取和写入权限，但对 File2 只有读取权限，如图 8.3 所示。

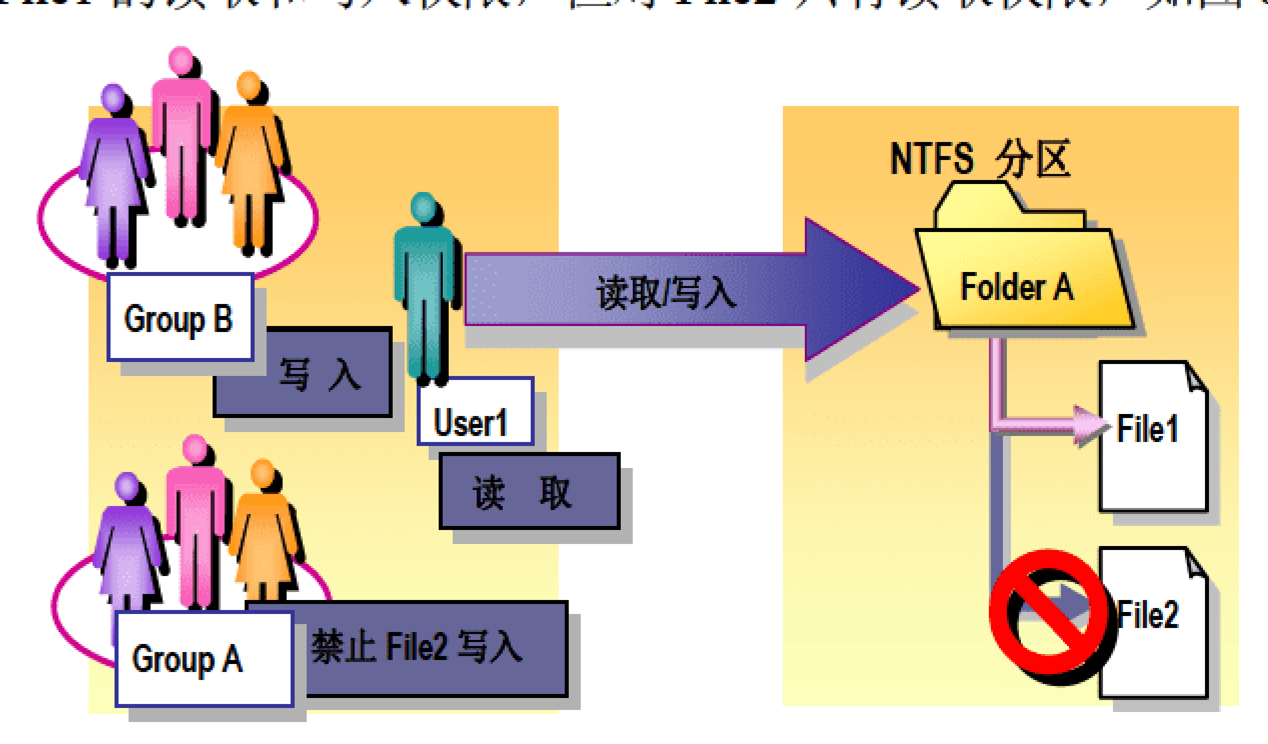


图 8.3　拒绝权限优先于其他权限

8.1.4　NTFS 权限的继承性

默认情况下，NTFS 权限是具有继承性的。所谓继承性，就是指 NTFS 权限自动从父对象传播到当前对象的过程，例如子文件夹继承来自其父文件夹的 NTFS 权限，文件继承来自文件夹的 NTFS 权限等。当然，正是因为 Windows 系统默认启用了 NTFS 权限继承，才会使用户不容易更加直观判断对象最终的 NTFS 权限值。管理员可以根据实际情况，限制这种权限继承。

1. 权限继承

文件和子文件夹从其父文件夹继承权限，即管理员为父文件夹指定的任何权限，同时也适用于该父文件夹中所包含的子文件夹和文件。当为一个 NTFS 文件夹指定权限时，不仅为该文件夹及其中所包含的文件和子文件夹指定了权限，同时也为将来在该文件夹中创建所有新文件和文件夹指定了权限。默认情况下，所有文件夹和文件都会自动从其父文件夹继承权限。

例如，当允许权限继承时，为 Folder1 设置的访问权限，将自动被传递给 File1、Folder2 和 File2。也就是说，子文件夹 Folder2 和文件 File1、File2 将自动取得为父文件夹 Folder1 设置的访问权限，如图 8.4 所示。

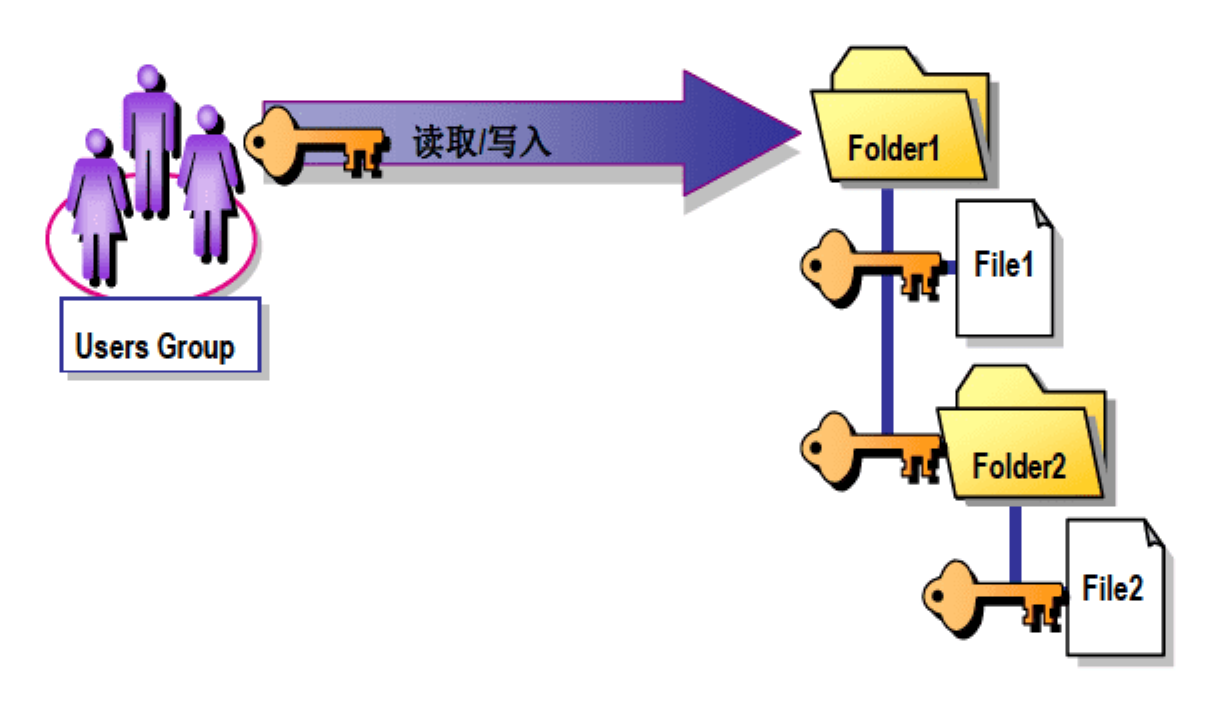


图 8.4　权限继承

2. 禁止权限继承

可以禁止指定给一个父文件夹的权限被这个文件夹中所包含的子文件夹和文件继承。也就是说，子文件夹和文件不会继承指定给包含它们的父文件夹的权限。被禁止继承权限的文件夹

变成新的父文件夹，为该文件夹指定的权限将会被它所包含的任何子文件夹和文件继承。

例如，当禁止权限继承时，为 Folder1 设置的访问权限，将不被传递给 File1、Folder2 和 File2。也就是说，子文件夹 Folder2 和文件 File1、File2 不能自动取得为父文件夹 Folder1 设置的访问权限，必须一一为这些子文件夹和文件分别设置访问权限，示意图如图 8.5 所示。

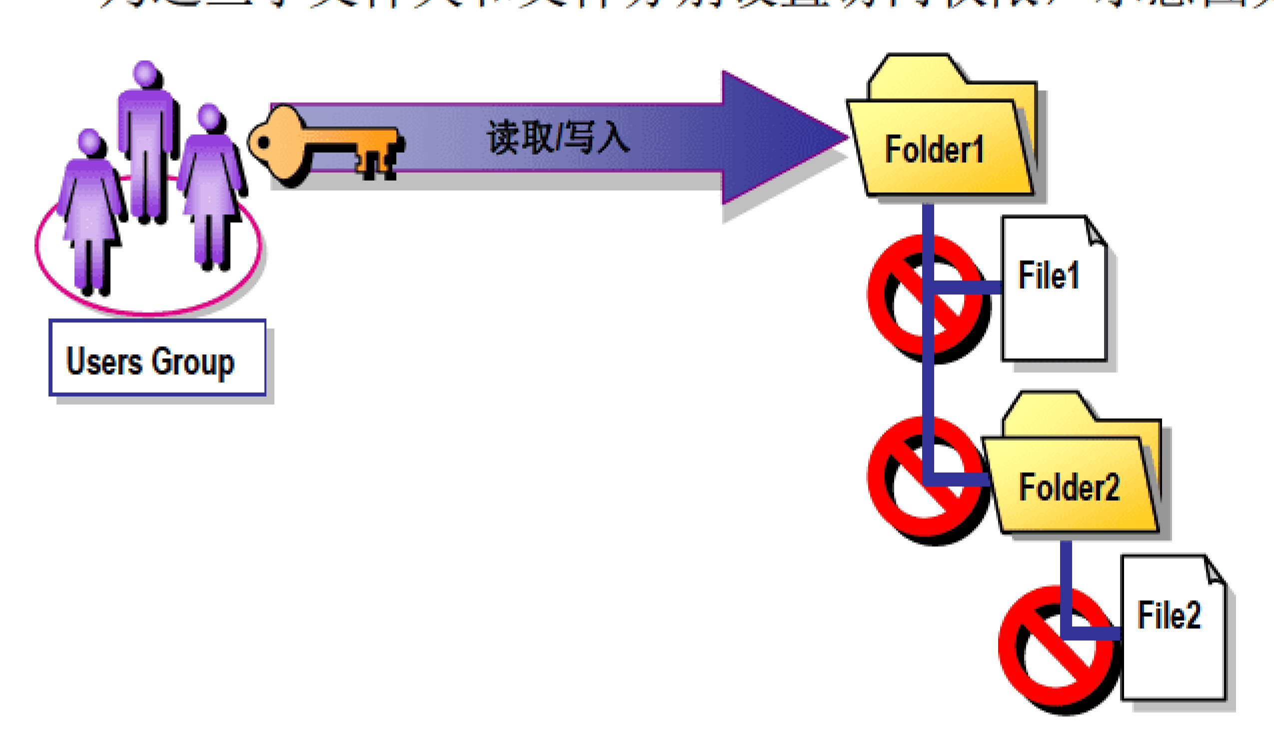


图 8.5　禁止继承权限

8.1.5　设置磁盘根目录访问权限

NTFS 权限是可以继承的，而默认情况下磁盘根目录的权限设置将自动播发到其所包含的所有子文件和文件夹上，因此对于根目录的访问权限控制是至关重要的。另外，为了便于对某分区上的所有文件和文件夹访问权限进行统一部署，也可以直接对磁盘根目录操作。

01 打开“Windows 资源管理器”窗口，右击“本地磁盘（C:）”选择快捷菜单中的“属性”选项，显示如图 8.6 所示“本地磁盘（C:）属性”对话框，切换到“安全”选项卡。

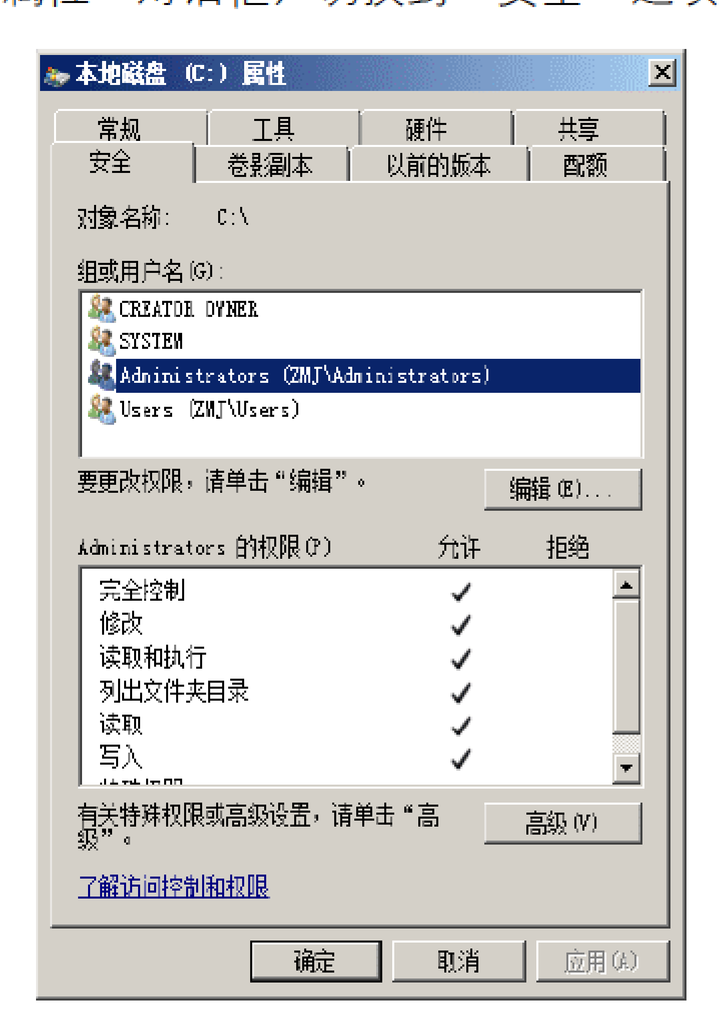


图 8.6　“本地磁盘（C:）属性”对话框

02 单击“高级”按钮，显示如图 8.7 所示“本地磁盘（C:）的高级安全设置”对话框。在“权限项目”列表中，选择希望修改权限设置的用户帐户或组。

03 单击“编辑”按钮，显示如图 8.8 所示权限设置对话框，选中“使用可从此对象继承的权限替换所有后

代上现有的所有可继承权限”复选框。



图 8.7　“本地磁盘（C:）的高级安全设置”对话框



图 8.8　权限设置对话框

04 单击“确定”按钮，回到“本地磁盘（C:）的高级安全设置”对话框，单击“确定”按钮。回到“本地磁盘（C:）属性”对话框，再次单击“确定”按钮即可完成设置权限的操作。

8.1.6　取消 Everyone 组所有权限

Everyone 组是 Windows 系统中的一个特殊组，代表所有当前系统或网络上的所有用户帐户，包括来自其他域或网络计算机的来宾帐户，并且无论用户何时登录到网络上，或通过网络访问本地计算机，都会自动将该用户添加到 Everyone 组中。如果为 Everyone 组赋予某种控制权限，则任何用户都可以对所涉及的文件夹或文件进行操作，严重影响系统安全，因此建议取消 Everyone 组的所有权限。需要注意的是，在早期版本的 Windows NT 系统中，匿名登录用户也是属于 Everyone 组的，但在 Windows Server 2003/2008 系统中，“匿名登录”组在默认情况下已不是 Everyone 组的成员。

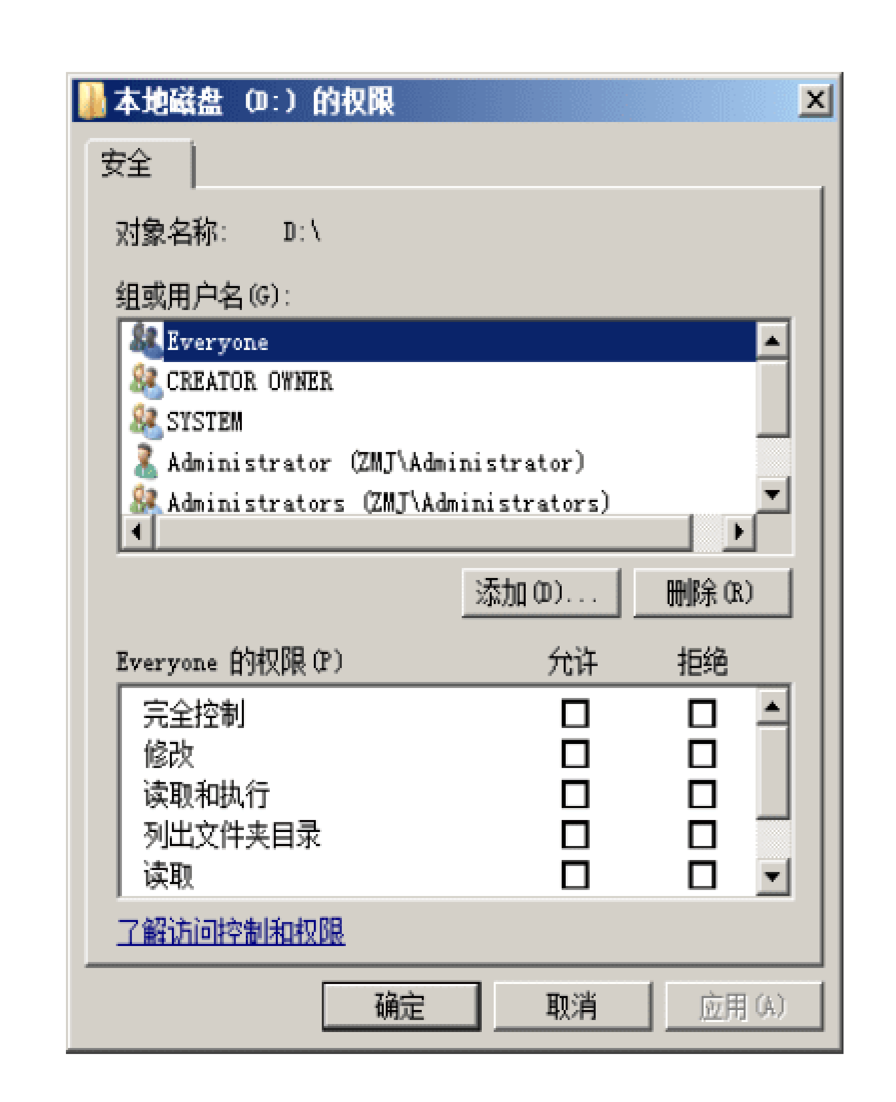


图 8.9　“本地磁盘（D:）的权限”对话框

打开“Windows 资源管理器”，右击“本地磁盘（D:）”盘符选项，在弹出的快捷菜单中选择“属性”命令，打开“本地磁盘（D:）属性”对话框。选择“安全”选项卡，单击“编辑”按钮，显示如图 8.9 所示“本地磁盘（D:）的权限”对话框，在“组或用户名”列表框中选中“Everyone”，单击“删除”按钮将其删除。最后，单击“确定”按钮保存设置即可。

默认情况下，在 Windows Server 2008 系统中，Everyone 组只被赋予了很少的读取权限，安全性相对较高。

8.2 文件夹共享安全

为了防止网络用户恶意删除或修改共享文件，管理员可以为不同的用户帐户赋予不同的访问权限，只允许少量用户具备修改或删除权限，普通用户授予其“只读”权限即可。隐藏共享，可以只允许指定的用户浏览共享资源，增加了共享资源的安全性。

8.2.1 创建共享文件夹

除系统默认设置的共享目录外，用户还可以根据需要随时设置共享文件夹。另外，在文件服务器上，发布新的共享资源时，也需要将所在目录设置为共享。在 Windows Server 2008 系统中，用户可以通过如下几种方法设置共享文件夹。

1. 方法一：“计算机管理”控制台

01 选择“开始”→“管理工具”→“计算机管理”命令，打开“计算机管理”对话框。依次选择“计算机管理（本地）”→“共享文件夹”，右击“共享”命令，在弹出的快捷菜单中选择“新建共享”命令，显示“创建共享文件夹向导”对话框。依次单击“下一步”按钮，设置源文件夹路径和共享名，如图 8.10 所示。

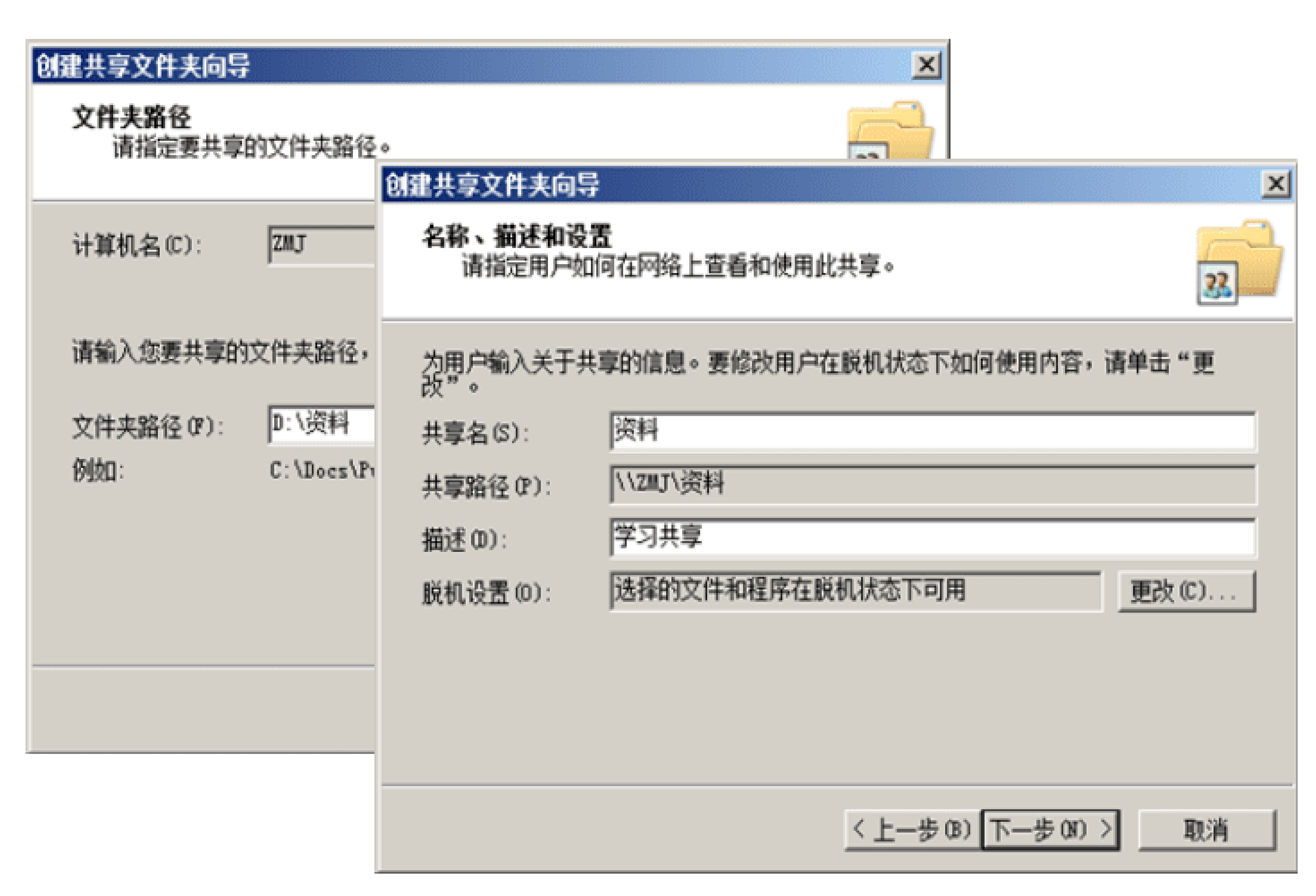


图 8.10 设置源文件夹路径和共享名

02 单击“下一步”按钮，显示共享文件夹的权限设置对话框，选择“所有用户有只读访问权限”单选按钮。单击“完成”按钮，显示共享成功窗口，如图 8.11 所示。

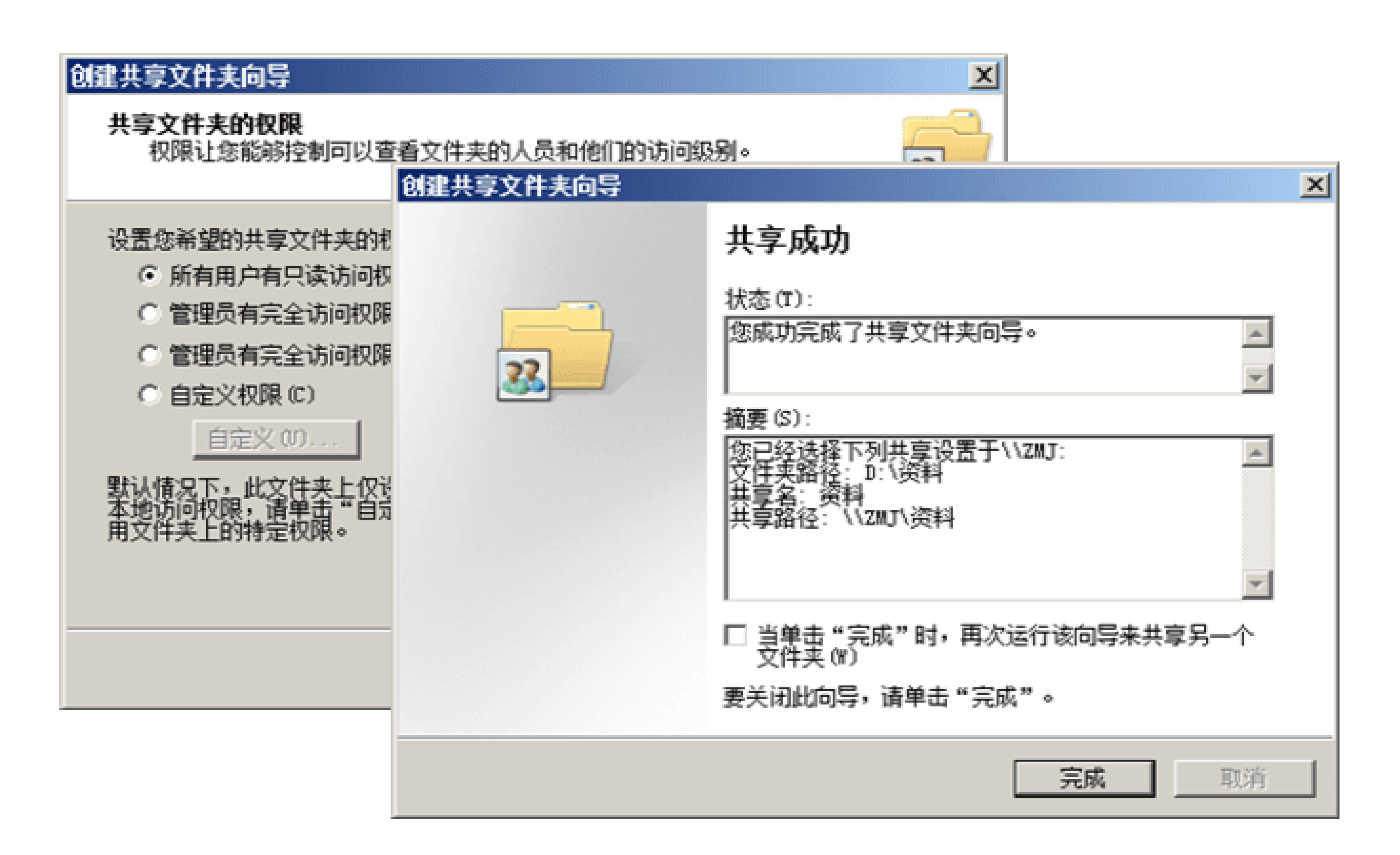


图 8.11　设置共享文件夹的权限

03 单击“完成”按钮，根据所选择的路径打开共享文件夹的路径，即可看到选择的文件夹已经共享，如图 8.12 所示。

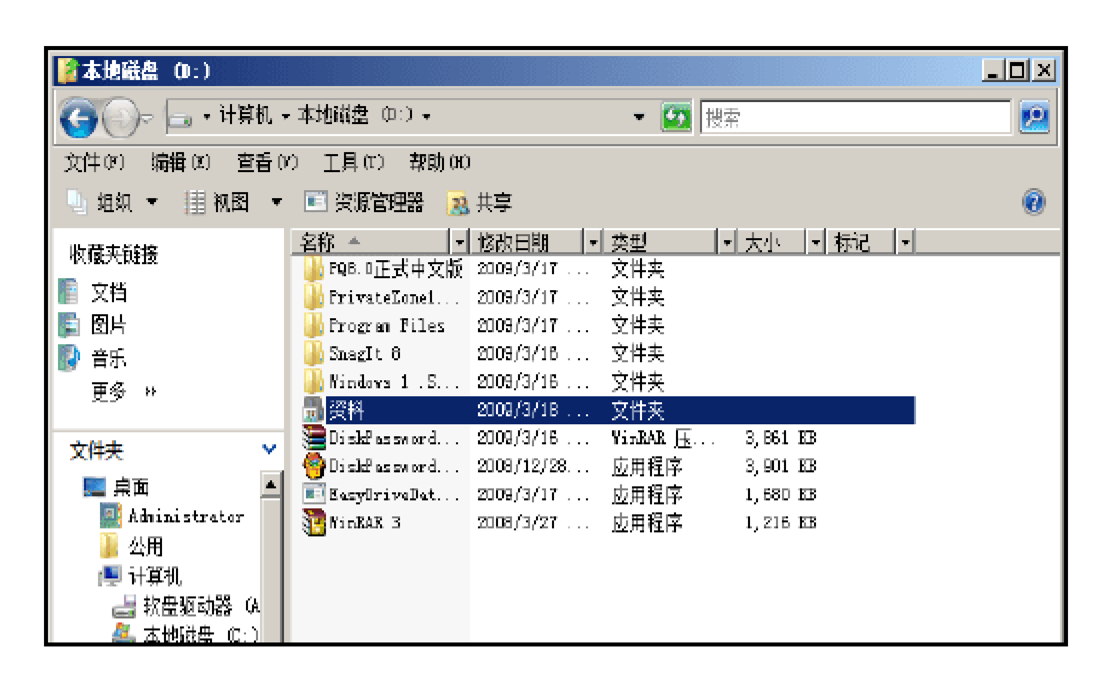


图 8.12　“资料”文件夹已共享

2. 方法二：“文件共享”向导

01 在“Windows 资源管理器”窗口中，右击“学习”文件夹，选择快捷菜单中的“共享”选项，显示如图 8.13 所示“文件共享”对话框。

02 在下拉列表项内选择要与其共享的网络上的用户，单击“添加”按钮，将其添加到下方列表中，单击“共享”按钮，显示完成共享对话框，如图 8.14 所示。



图 8.13　“文件共享”对话框



图 8.14　完成共享

03 单击“完成”按钮，根据所选择的路径打开共享文件夹的路径，即可看到选择的文件夹已经共享。

3. 方法三：“高级共享”向导

在“Windows 资源管理器”窗口中，右击需要共享的文件或文件夹（仍以“学习”文件夹为例），选择快捷菜单中的“属性”选项，显示“学习 属性”对话框，切换到“共享”选项卡。单击“高级共享”按钮，显示“高级共享”对话框，如图 8.15 所示。选中“共享此文件夹”复选框，并在“将同时共享的用户数量限制为:”微调框内设置适当的用户数量。最后，依次单击“确定”按钮，保存设置即可。

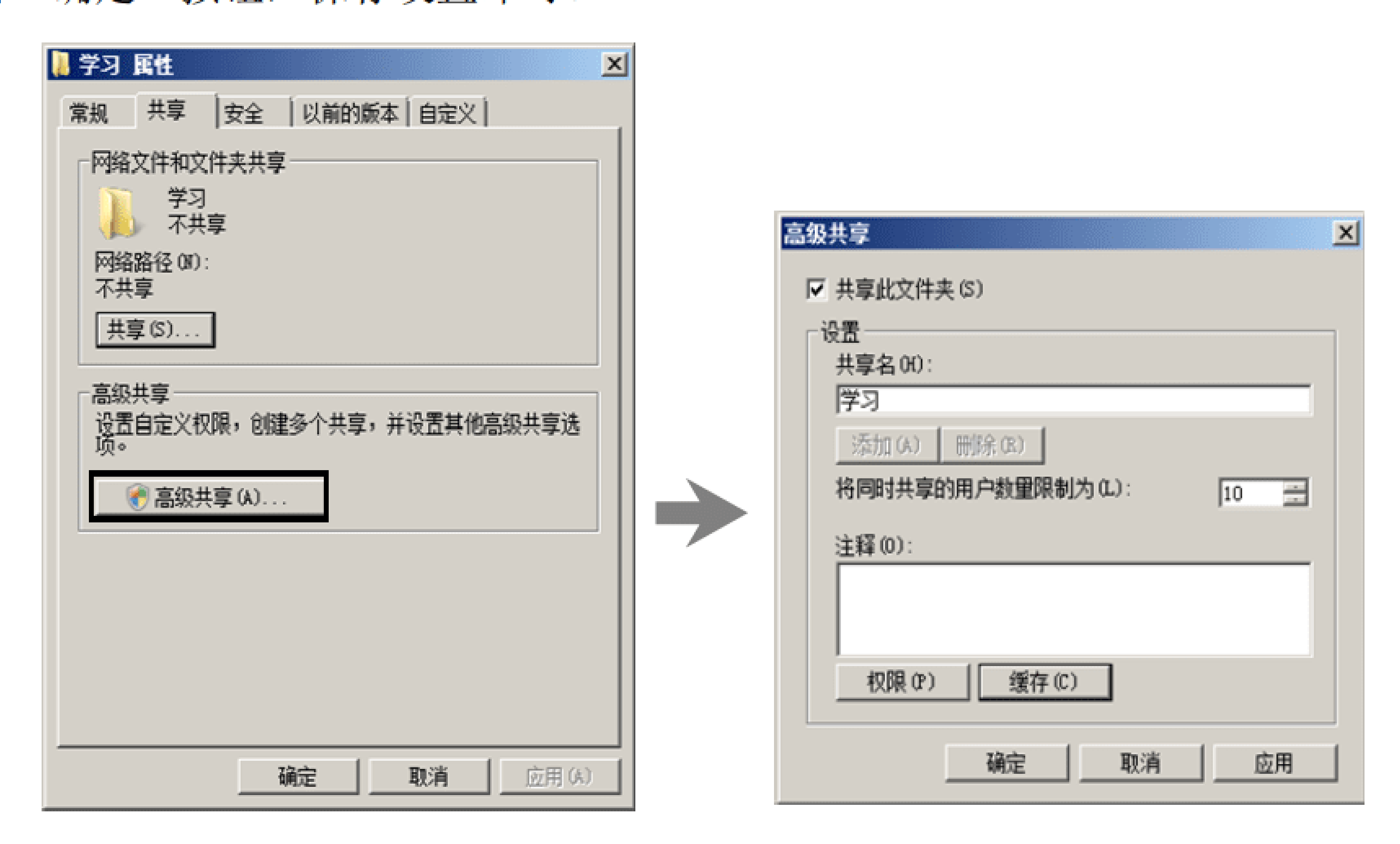


图 8.15　设置高级共享属性

“高级共享”对话框中各选项或按钮的含义如下：

- “将同时共享的用户数量限制为”选项用于限制共享用户的上限，确保在为网络用户提供共享的同时，不至于影响本地正常应用；
- 单击“权限”按钮，可以针对不同的用户帐户，设置不同的共享访问权限，系统默认的是对所有文件夹设置了所有用户具有“读取”的最基本共享权限；
- 单击“缓存”按钮，可以设置当前共享文件夹是否允许用户脱机访问，可以根据实际需要只允许脱机访问指定的文件或应用程序。

4. 方法四：net share 命令

以管理员身份打开“命令提示符”窗口，使用 net share 命令，也可以设置共享文件夹。仍以“E:\学习”为例，在命令提示符窗口中，输入如下命令：

```
net share e:\学习
```

回车执行，即可将“学习”文件夹设置为共享。继续输入 net share，按下 Enter 键，即可显示共享的文件夹，如图 8.16 所示。

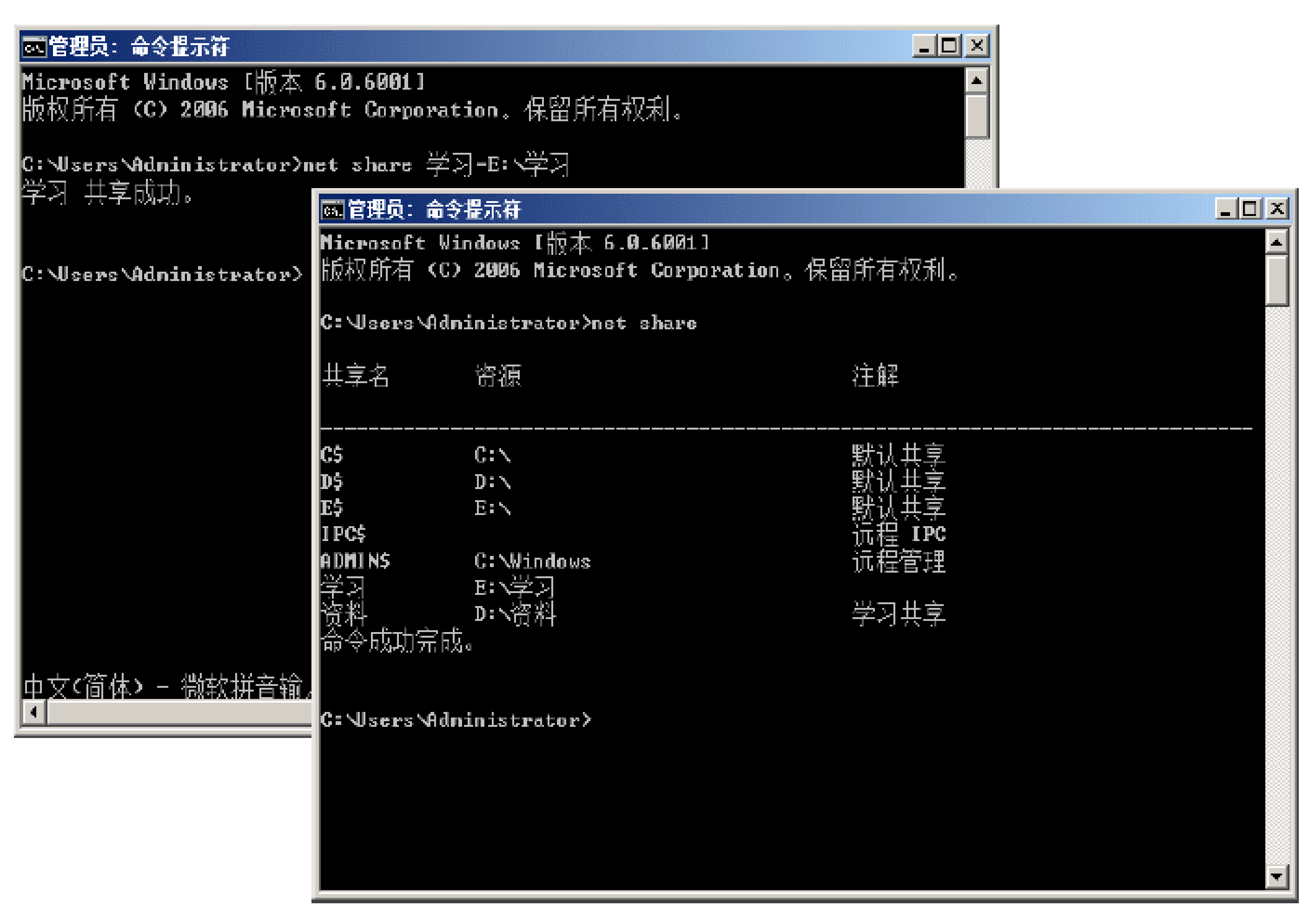


图 8.16　使用 net share 创建共享文件夹



提示　net share 是创建、删除、管理和显示共享资源的命令；sharename=drive:path 参数是用来指定共享资源的网络名称和其绝对路径的。

8.2.2　共享文件夹的权限

为了保护计算机及其资源的安全，必须考虑用户将拥有的权利。可通过授权用户或组特定的用户权利来确保某计算机或多台计算机的安全。可以通过分配用户或组的权限对该对象执行特定操作来保护对象。共享的权限只能控制网络访问，不能控制本机访问。Windows Server 2008 提供的共享权限设置包括：

- 完全控制。完全控制权限是指派给本地计算机上的 Administrators 组的默认权限。“完全控制”权限具有全部读取及更改权限；
- 更改权限。“更改”权限不是任何组的默认权限。“更改”权限除允许以上所有的“读取”权限外，还具有如下权限：
  - 添加文件和子文件夹；
  - 更改文件中的数据；
  - 删除子文件夹和文件。
- 读取权限。“读取”权限是指派给 Everyone 组的默认权限。“读取”权限允许进行下面的操作：
  - 查看文件名和子文件夹名；
  - 查看文件中的数据；
  - 运行程序文件。

8.2.3 停止默认共享文件夹

默认共享主要是为了方便网络管理员管理网络中的计算机，特别是在基于域的网络中，专门有几个默认共享用于存储用户配置文件，是非常方便的。但是，默认共享在方便管理的同时，也给计算机的安全埋下了重大安全隐患。如果知道了管理员帐户和密码，任何人都能访问计算机，所以如果管理员帐户密码恶意用户窃取，对于计算机的安全来说是非常不利的。如果在网络中没有使用默认共享的必要，建议用户将系统的默认共享关闭，从而进一步保证计算机的安全。

1. 使用 net share 命令

以管理员身份打开“命令提示符”窗口，在命令行提示符下，输入如下命令：

```
NET SHARE Admin$ /DELETE
```

按 Enter 键，命令成功执行，即可停止共享，如图 8.17 所示。

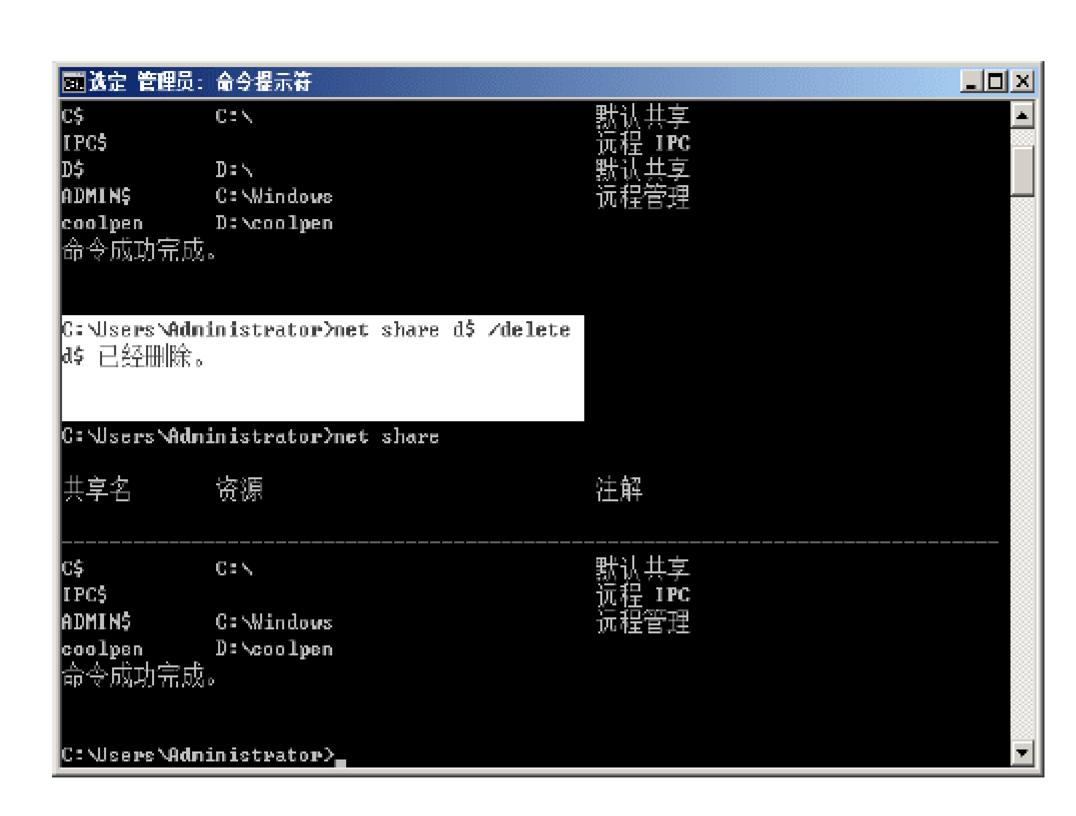


图 8.17 删除 d$默认共享

其中 d$表示系统默认共享 D 盘，其他如 C$、ADMIN$、IPC$等都可以使用此种格式删除。

在“/delete”前必须要有空格。可以使用“NET SHARE ADMIN$”或“NET SHARE IPC$”建立“ADMIN$”或“NET SHARE IPC$”共享（如果共享存在，则为显示共享），但需要注意的是，其他共享则不能使用该方法来建议默认共享。

如果需要删除所有的默认共享，可以使脚本命令（批处理文件方式）完成（即扩展名为“.bat”的文件）：

```
net share IPC$ /delete
net share Admin$ /delete
net share C$ /delete
net share D$ /delete
......
```

可以根据需要分别删除默认共享的盘符，该批处理文件可以在命令提示符下运行，也可以将其添加到启动项中，如图 8.18 所示。这里创建一个名为“share.bat”的批处理文件，用以将系统的默认共享删除，并在命令提示符下运行。

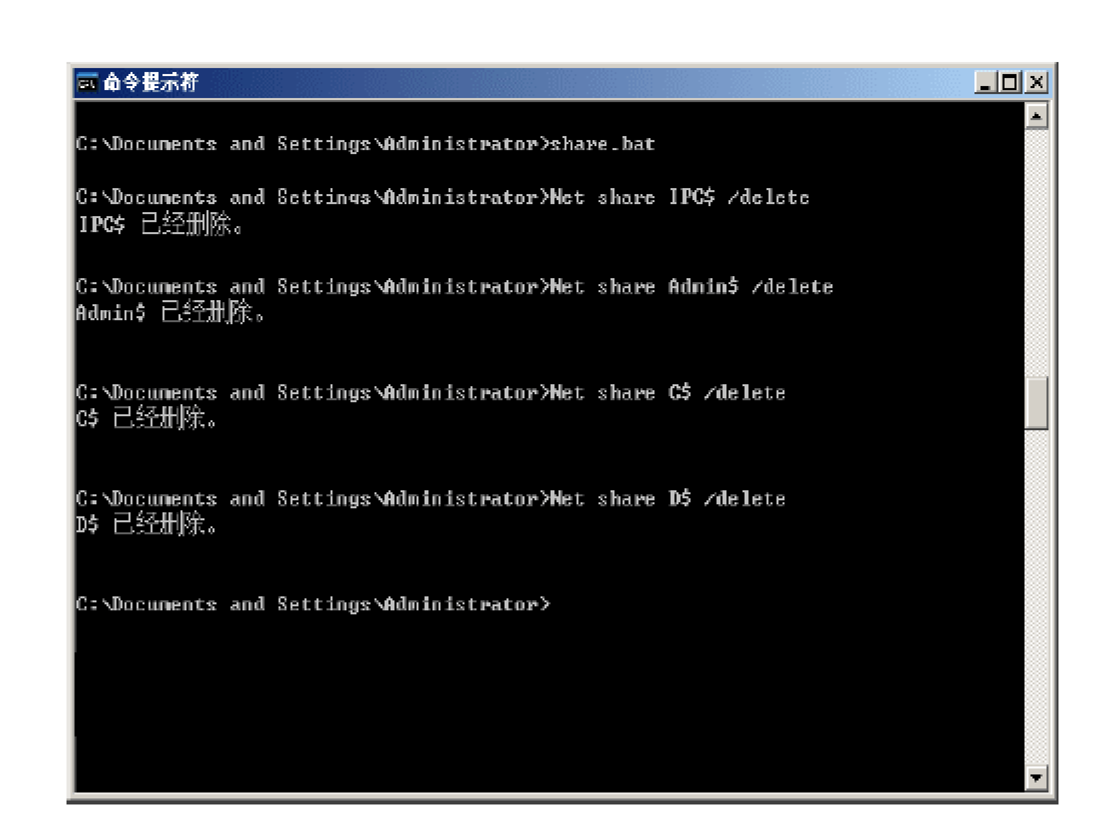


图 8.18 在命令提示符下运行批处理文件

2. 关闭 Server 服务

共享使用的是计算机系统的 Server 服务，如果将该服务直接关闭，就可以直接删除默认共享。

依次选择“开始”→“管理工具”→“服务”命令，打开“服务”窗口，双击“Server”服务命令，打开“Server 的属性（本地计算机）”对话框。在“启动类型”下拉列表中，选择“手动”命令，以免再次重新启动系统时服务随之启动。单击“停止”按钮，即可停止“Server”服务如图 8.19 所示。

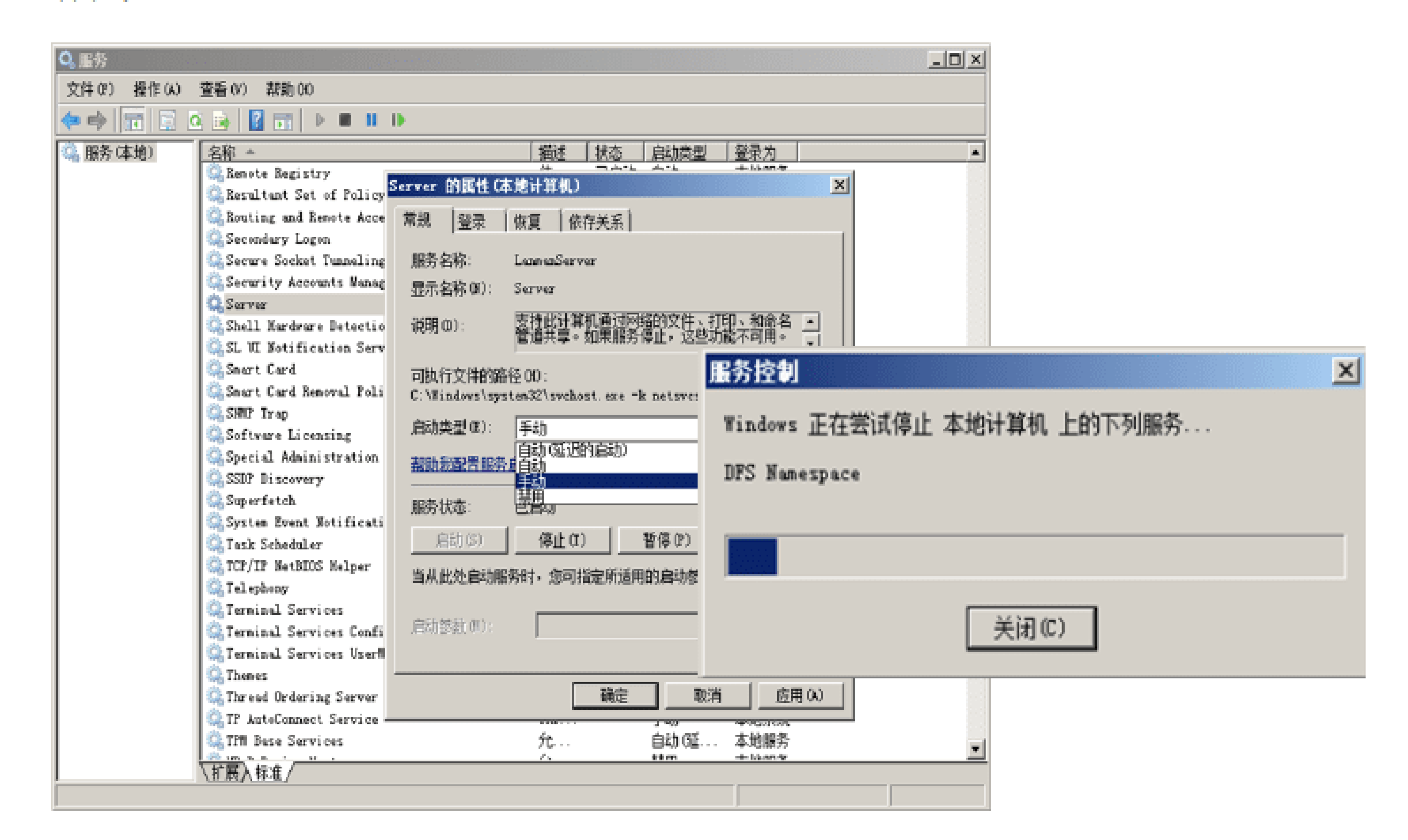


图 8.19　关闭 Server 服务

再次打开命令提示符窗口，输入“net share”字符串命令，按下回车键，显示如图 8.20 所示结果，提示 Server 服务没有启动，直接输入“n”并回车即可。

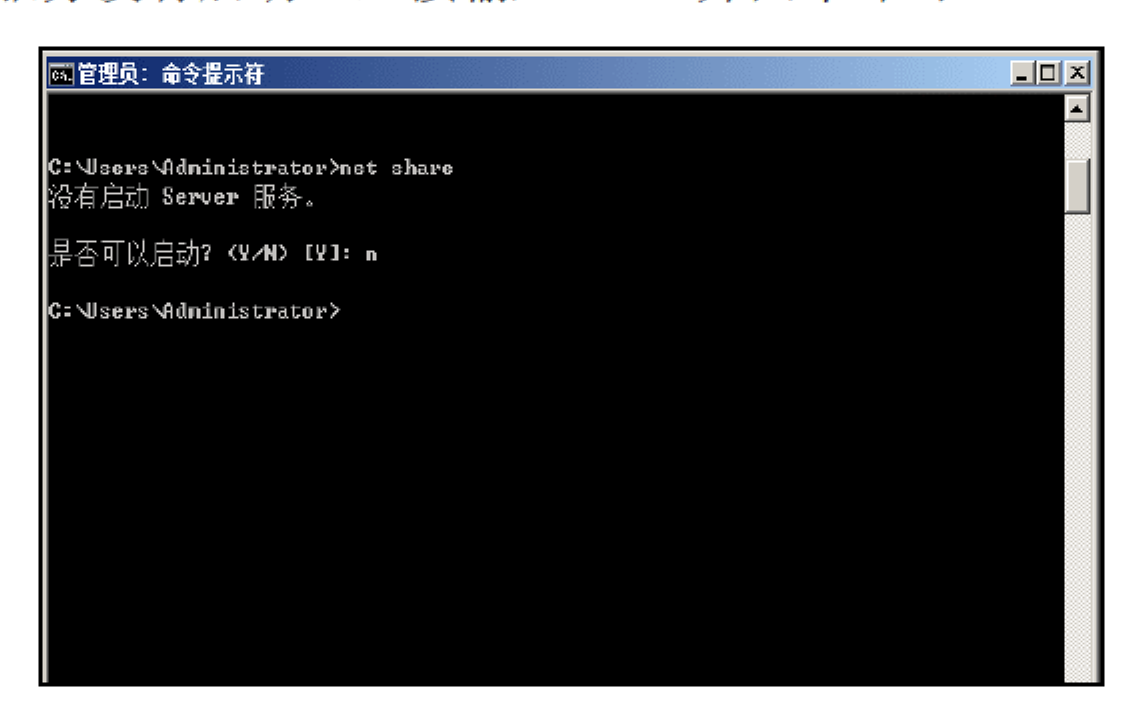


图 8.20　关闭 Server 服务后

使用这种方法停止默认共享后，其他共享也将同时被取消，应慎重选择。

3. 修改注册表

使用前面两种方法停止完成系统默认共享，当系统重新启动后，默认共享会重新恢复。如果用户需要永久性地停止系统默认共享，可以通过修改注册表的方法来实现该目的。停止系统默认共享的键值，默认情况下在 Windows 操作系统上不存在，需要用户手动添加该键值，修改后重新启动计算机即可使该键值生效。

01 单击“开始”按钮，在“开始搜索”文本框中，输入“regedit”并按下回车键，打开“注册表编辑器”窗口。选择如下注册表子项：[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\AutotunedParameters]，如图 8.21 所示。

02 右击右侧的空白窗口处，在弹出的快捷菜单中选择“新建”命令，在子菜单中选择“Dword 值”命令，新建一个名为“AutoShareServer”的 DWORD 值，并将其赋值为：00000000，如图 8.22 所示。

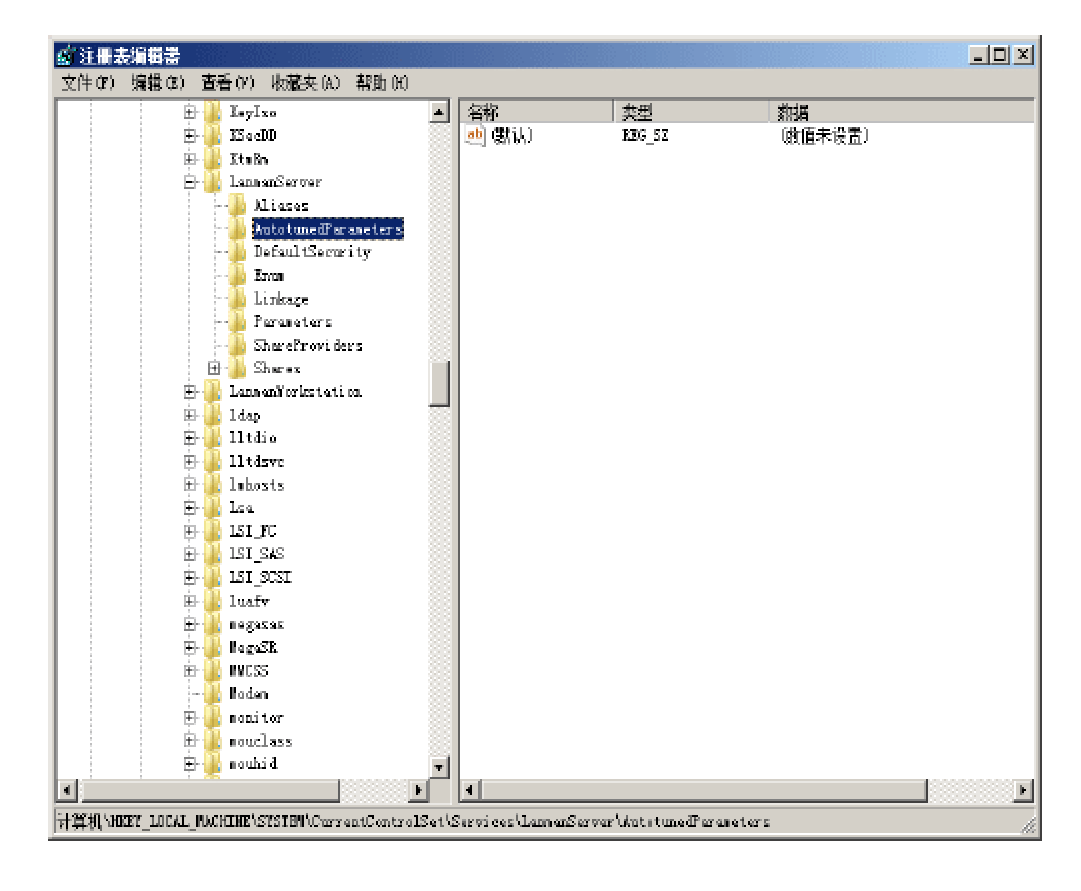


图 8.21　展开的注册表项目

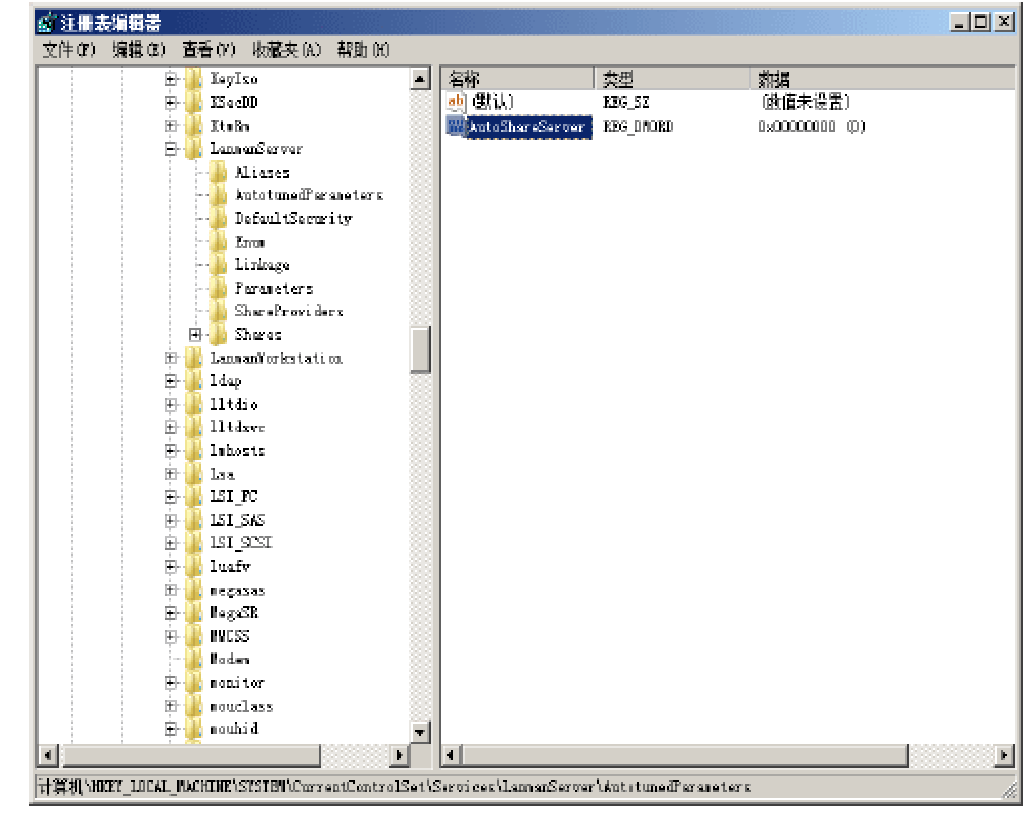


图 8.22　创建 DWORD 值

4. Microsoft 网络的文件和打印机共享

除使用修改注册表的方法外，还可以使用卸载网卡相关属性的方法，关闭默认共享。

在“控制面板”窗口中，打开“网络和共享中心”窗口。单击“查看状态”链接，打开“本地连接 状态”对话框，单击“属性”按钮，显示如图 8.23 所示“本地连接 属性”对话框。

选中“Microsoft 网络的文件和打印机共享”复选框，单击“卸载”按钮，系统提示确认删除信息，显示如图 8.24 所示“卸载 Microsoft 网络的文件和打印机共享”对话框。单击“是”按钮，即可完成“Microsoft 网络的文件和打印机共享”项目的卸载。

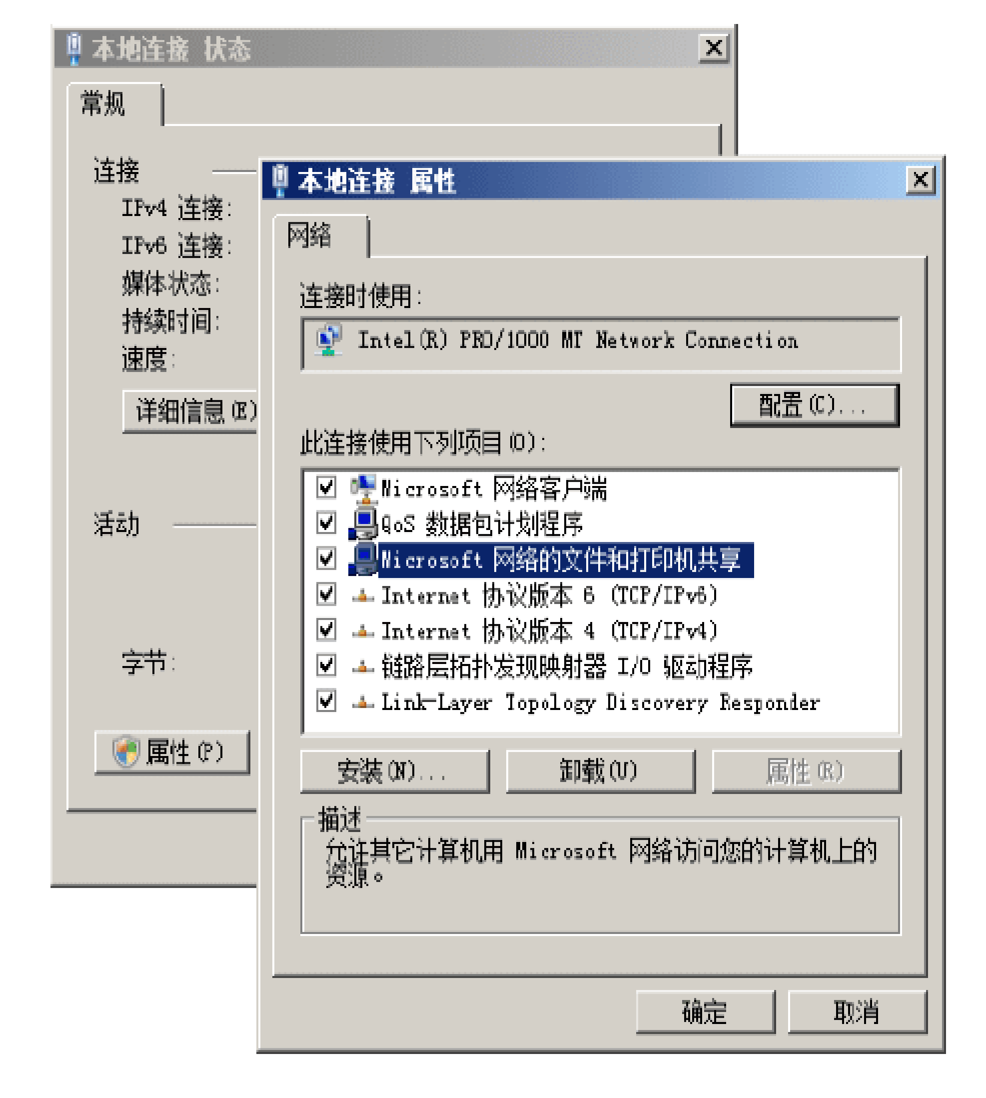


图 8.23　设置本地连接属性

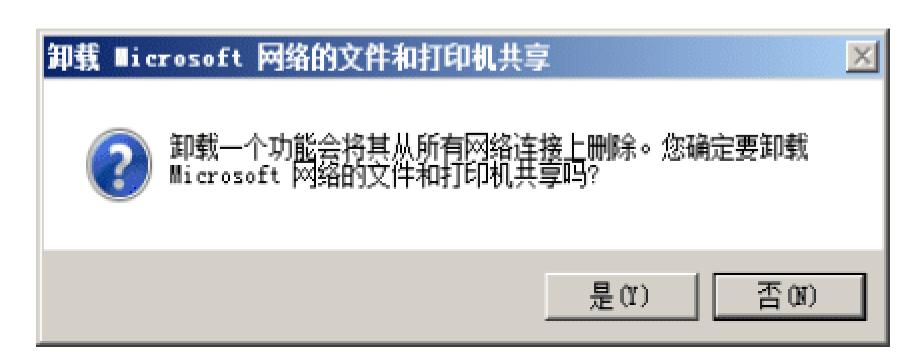


图 8.24　卸载信息提示

8.2.4　设置隐藏共享

通常情况下，用户可以通过网上邻居查看或访问其他计算机上的共享资源，但其中并不包括隐藏共享。因此设置隐藏共享也是保护共享资源安全的一种常用方法，访问者必须使用准确的共享名才可以访问。

在“Windows 资源管理器”中，右击想要设置隐藏共享的文件夹（以 book 文件夹为例），并选择快捷菜单中的“属性”，打开“book 属性”对话框，切换至“共享”选项卡，单击“高级共享”按钮，打开如图 8.25 所示“高级共享”对话框。选中“共享此文件夹”复选框，并在“共享名”文本框中显示的默认名称后追加“$”，也可以设置其他共享名，但隐藏共享必须以“$”结尾。网络中的其他计算机无法直接通过资源管理器访问隐藏共享，但可以在任意地址栏中输入“\\服务器名\共享名”进行访问，注意此时的共享名中也包括特殊字符“$”，如“\\tjl\book$”。此外，也可以通过映射网络驱动器直接访问，如图 8.26 所示。

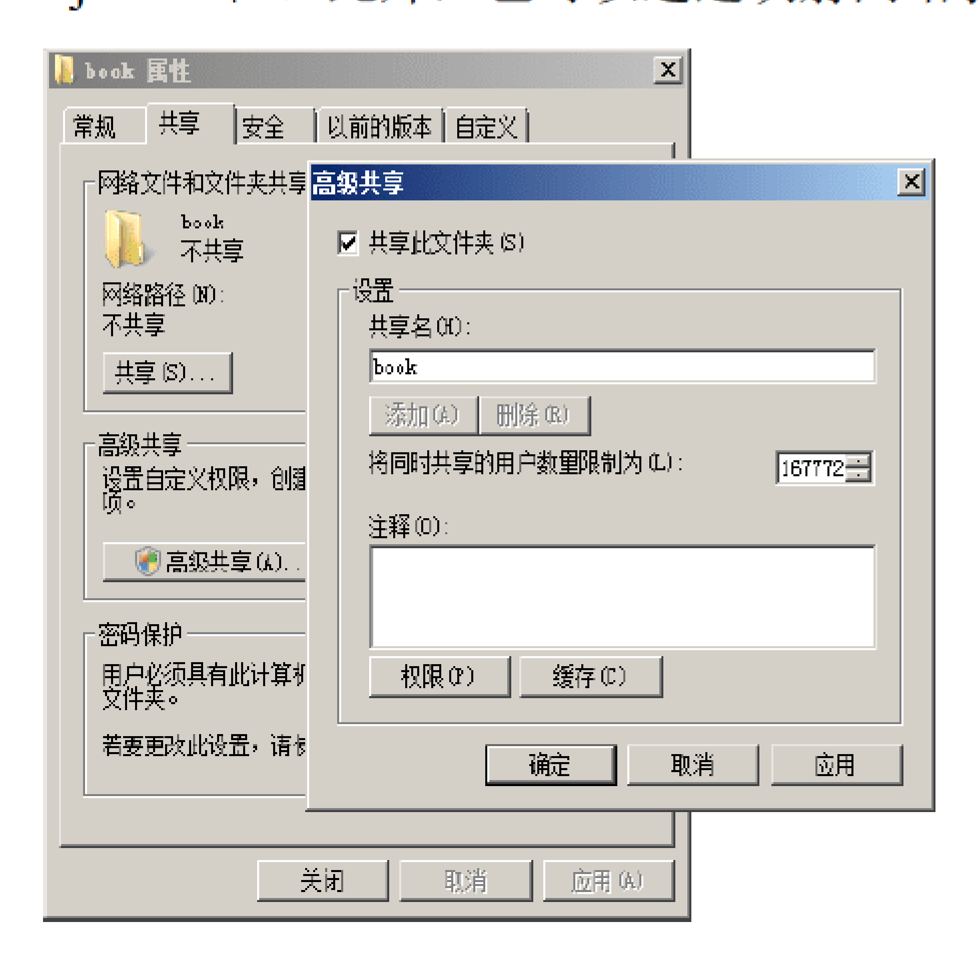


图 8.25　“高级共享”对话框

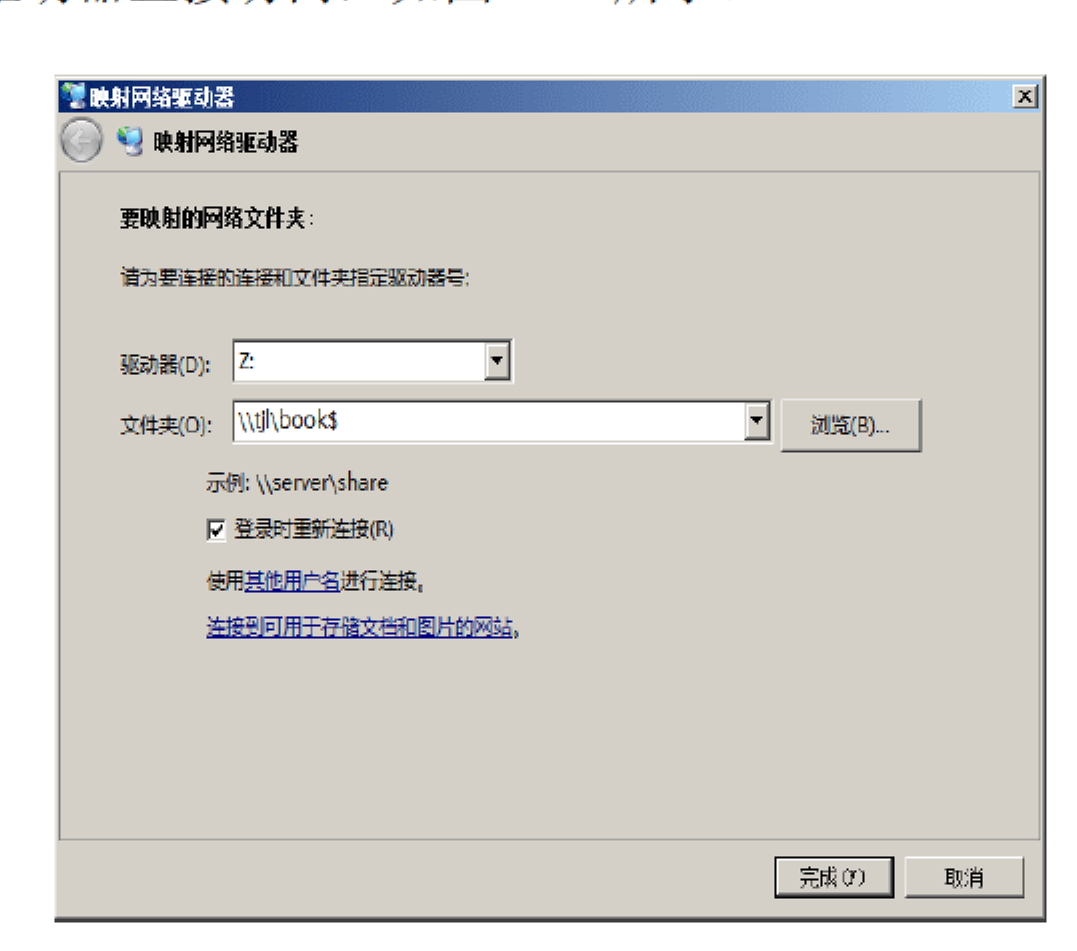


图 8.26　“映射网络驱动器”对话框

8.3　权限管理服务

威胁文件安全的主要因素往往来自内部用户，而普通的访问权限限定很难做到万无一失。Windows Server 2008 系统中的 AD RMS（Rights Management Services，权限管理服务）可以通过数字证书和用户身份验证技术对各种 Office 文档的访问权限加以限制，可以有效防止内部用户通过各种途径擅自泄漏机密文档内容，从而确保了数据文件访问的安全性。

8.3.1　安装 AD RMS 前的准备

相对于先前的 RMS 而言，AD RMS 不再是一个独立服务插件，已经成为 Windows 的一项

内置功能，并且包含了某些升级功能，直接在管理服务器窗口中启动安装向导即可轻松安装。为了确保安装过程顺利进行，开始之前应做好如下准备工作：

- 将计算机加入到域，或者提升为域的额外域控制器，或者子域；
- 使用具有域用户帐户登录，但不能使用 Administrator 帐户登录；
- 安装 IIS 服务和 ASP.Net 组件；
- 安装 MSMQ（消息队列）服务；
- 选择数据库。如果要使用独立数据库，需要安装 SQL Server。否则，可使用 AD RMS 的自带数据库；
- 安装之前，确认 http://uddi.microsoft.com 和 https://uddi.microsoft.com 在 Internet Explorer 中被添加至“受信任的站点”或“本地 Internet”。

8.3.2 安装 AD RMS 服务器

AD RMS 服务并不是 Windows Server 2008 系统默认安装的组件，需要用户手动添加。完成必要的准备工作后，即可开始安装 AD RMS 服务器。另外，用户也可以直接安装 AD RMS 服务器，如果安装向导检测到未安装的组件，会提示用户，此时通过选择相关命令即可一并完成准备组件的部署。

01 依次选择“开始”→“管理工具”→“服务器管理器”命令，打开“服务器管理器”窗口，在左侧窗格中选择“角色”命令，在右侧窗格中选择“添加角色”命令，显示“选择服务器角色”对话框。选中“Active Directory Rights Management Services”复选框，提示是否添加所需的角色服务和功能。如果在此之前，已经完成各项准备工作，则不会显示该对话框，如图 8.27 所示。



图 8.27 选择服务器角色



提示 操作之前应将使用的与用户帐户添加到本地计算机的“Administrators 组”中。不能使用 Administrator 用户帐户登录，否则就会显示如图 8.28 所示警告框，提示无法安装。



图 8.28 更改登录帐户

02 单击“添加必需的角色服务”按钮，选中“Active Directory Rights Management Services”复选框。单击“下一步”按钮，简要介绍 Active Directory 权限管理服务的作用以及功能。单击“下一步”按钮，显示如图 8.29 所示“选择角色服务”对话框。如果选中“联合身份验证支持”复选框，将同时安装 AD FS 或与当前域中已有的 AD FS 关联使用，它允许用户使用当前域和其他域之间经过联合身份验证的信任关系来建立用户标识，以及提供对其他组织创建的受保护信息的访问权限。不需要联合身份验证的用户建议不要选择该复选框。

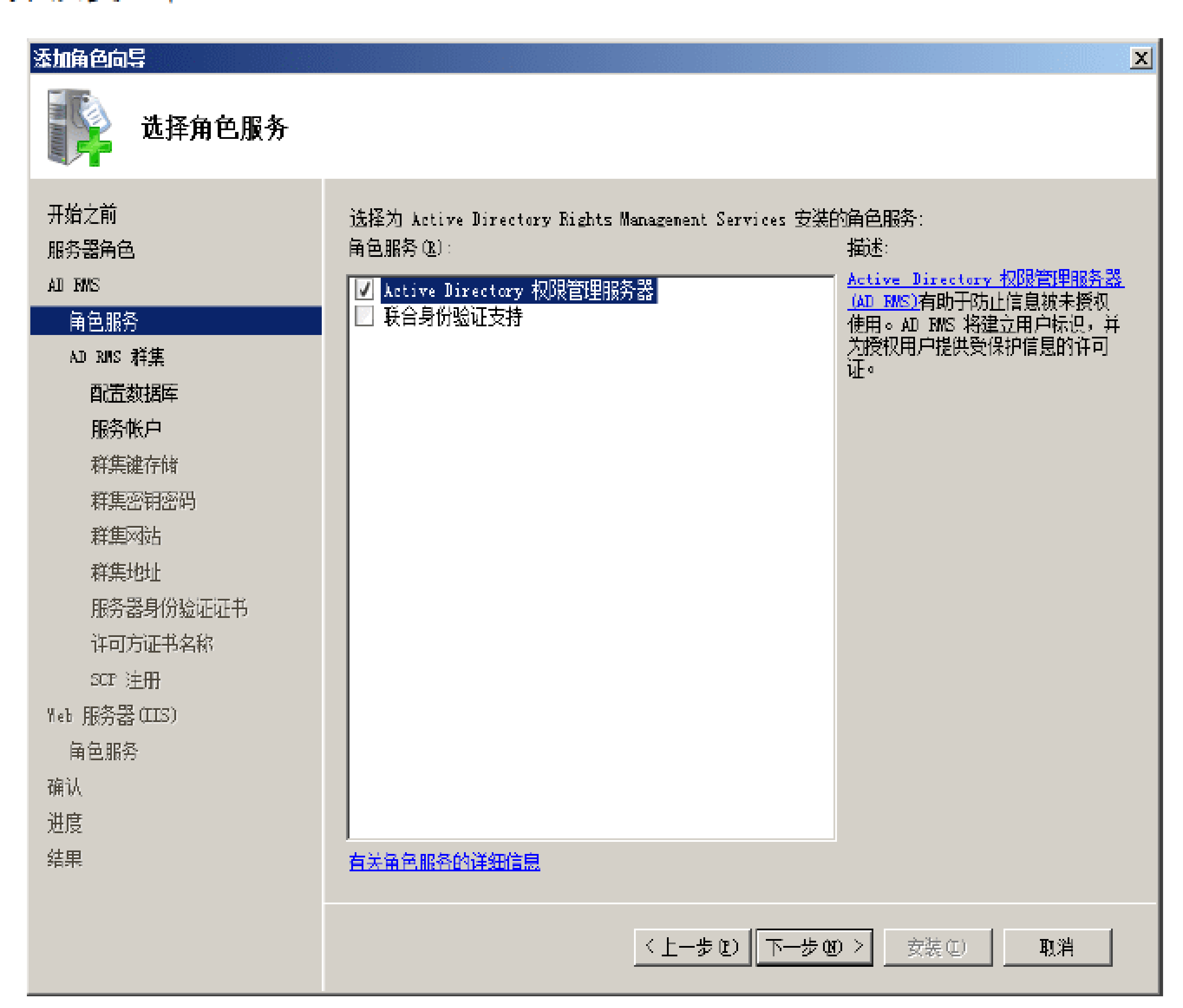


图 8.29 “选择角色服务”对话框

03 依次单击“下一步”按钮，设置 AD RMS 群集选项和数据库选项，如图 8.30 所示。在“创建或加入 AD RMS 群集”对话框中，系统默认选择“新建 AD RMS 群集”单选按钮，由于当前域中没有其他 AD RMS 群集可供加入，所以“加入现有 AD RMS 群集”单选按钮为灰色。安装完成后创建的第一台 AD RMS 服务器即为根群集，后来加入的 AD RMS 服务器为叶服务器。“选择配置数据库”对话框。如果网络中安装了 SQL Server 服务器，可选择“使用其他数据库服务器”单选按钮；如果要使用 AD RMS 自带的数据库，选择“在此服务器上使用 Windows 内部数据库”单选按钮即可。



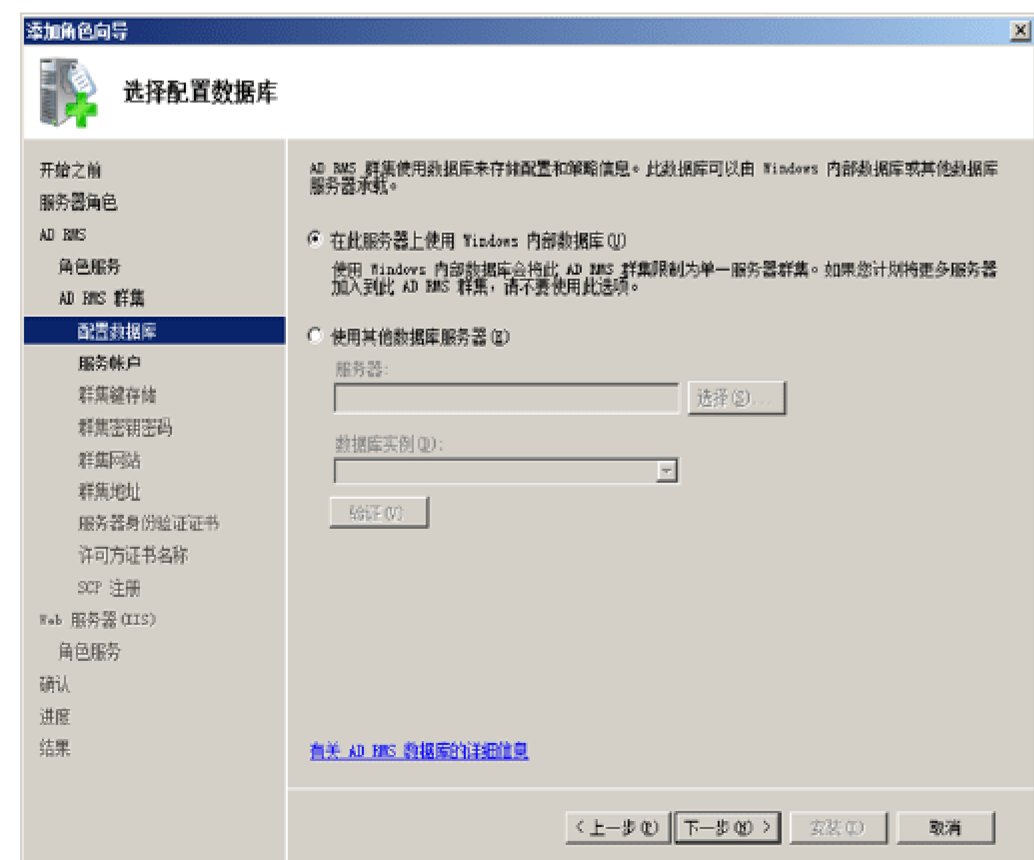


图 8.30　配置 AD RMS 群集和数据库

04 单击“下一步”按钮，显示如图 8.31 所示“指定服务帐户”对话框。该服务帐户也就是将来要在 AD RMS 群集中使用的帐户，可使用普通域成员帐户，但必须区别于当前服务器登录的域用户帐户。单击“指定”按钮，显示“Windows 安全”对话框，输入域用户帐户。单击“确定”按钮，域控制器会对提交的用户帐户和密码进行验证，如果正确无误则返回“指定服务帐户”对话框。

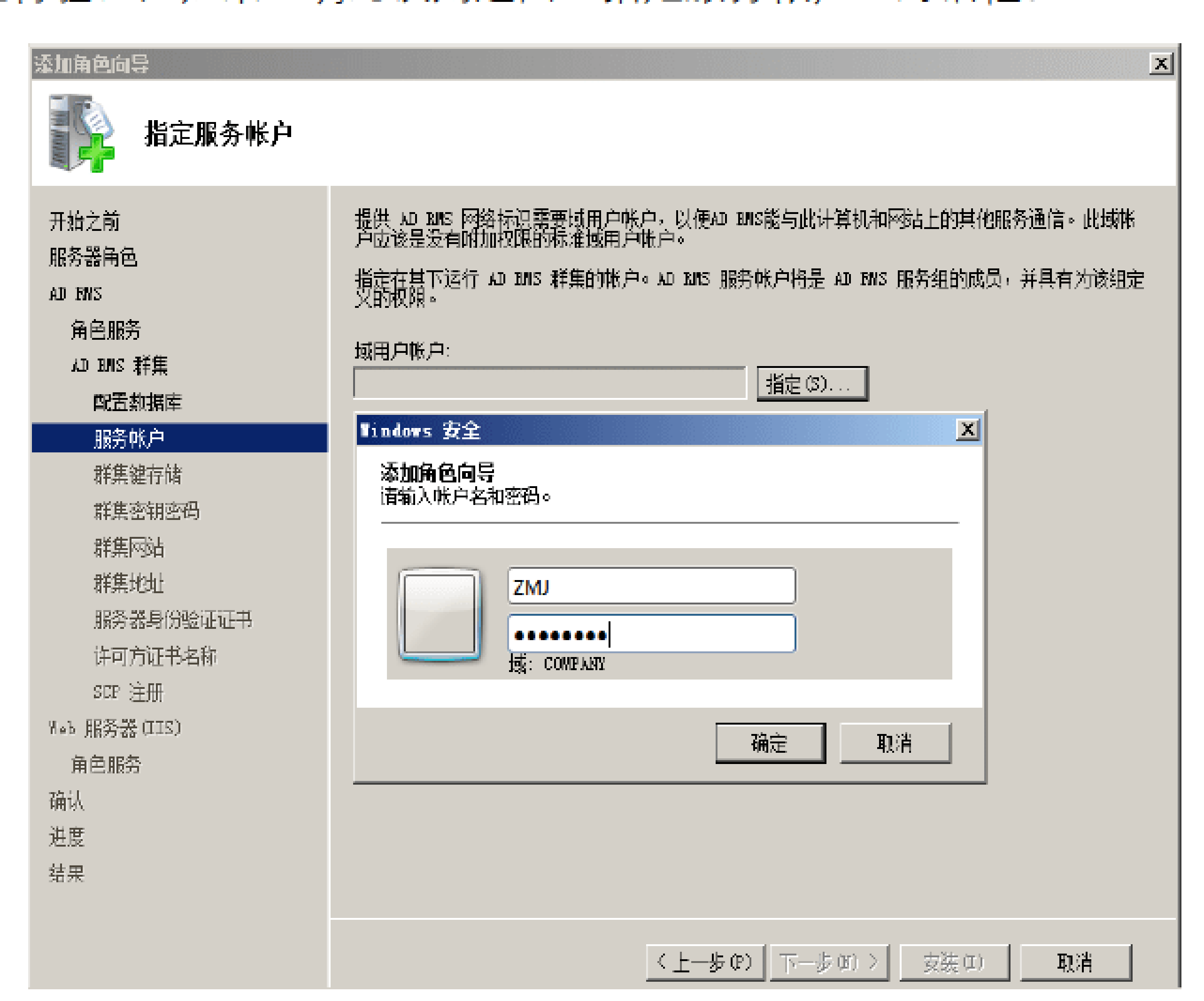


图 8.31　“指定服务帐户”对话框

05 依次单击“下一步”按钮，设置群集密钥存储方式和群集密钥密码，如图 8.32 所示。在“配置 AD RMS 群集键存储”对话框中，系统默认选择“使用 AD RMS 集中管理的键存储”单选按钮，即由本地服务器自动生成并存储密钥，这里选择该项，该密钥主要用于当前根服务器以及将来叶服务器的灾难恢复，必须牢记。在“指定 AD RMS 群集密钥密码”对话框中，其他 AD RMS 服务器加入群集时也要使用此密码，必须妥善保存。





图 8.32　设置群集键存储方式和群集密钥密码

06 依次单击“下一步”按钮，设置群集站点、地址和证书名称，如图 8.33 所示。在“选择 AD RMS 群集网站”对话框中，设置管理 AD RMS 群集服务器时使用的站点，保持默认即可。在“指定群集地址”对话框中，选择“使用未加密的连接”单选按钮，使用普通传输方式，输入域名，并单击“验证”按钮，确认不与其他站点冲突。在“命名服务器许可方证书”对话框中，系统默认会以计算机名命名证书，保持默认即可。

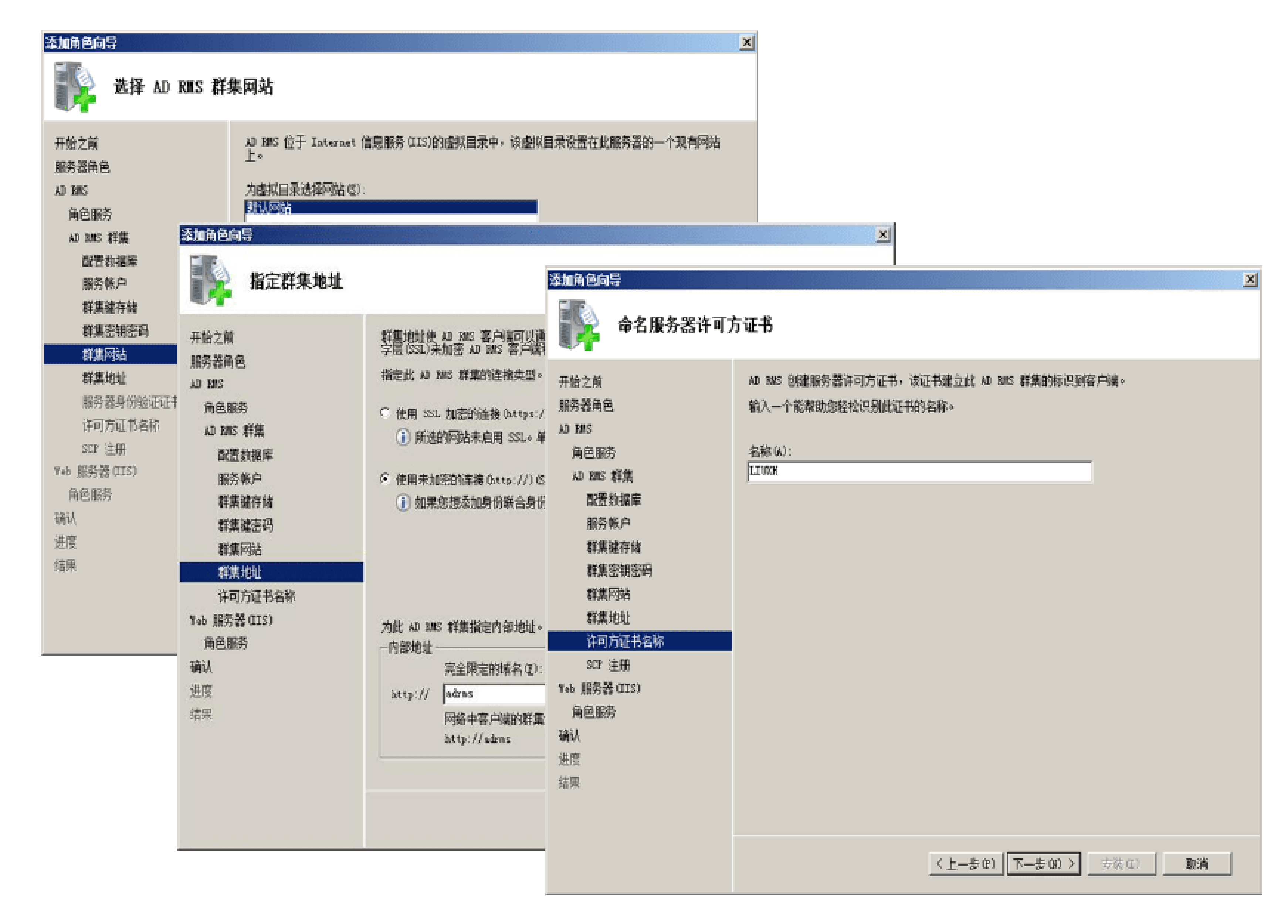


图 8.33　设置群集站点、地址和证书名称

07 依次单击“下一步”按钮，注册服务连接点并开始安装，直至安装完成，如图 8.34 所示。在“注册 AD RMS 服务连接点”对话框中，选择“立即注册 AD RMS 服务连接点”单选按钮，在安装完成后立即开始使用此 AD RMS 群集。

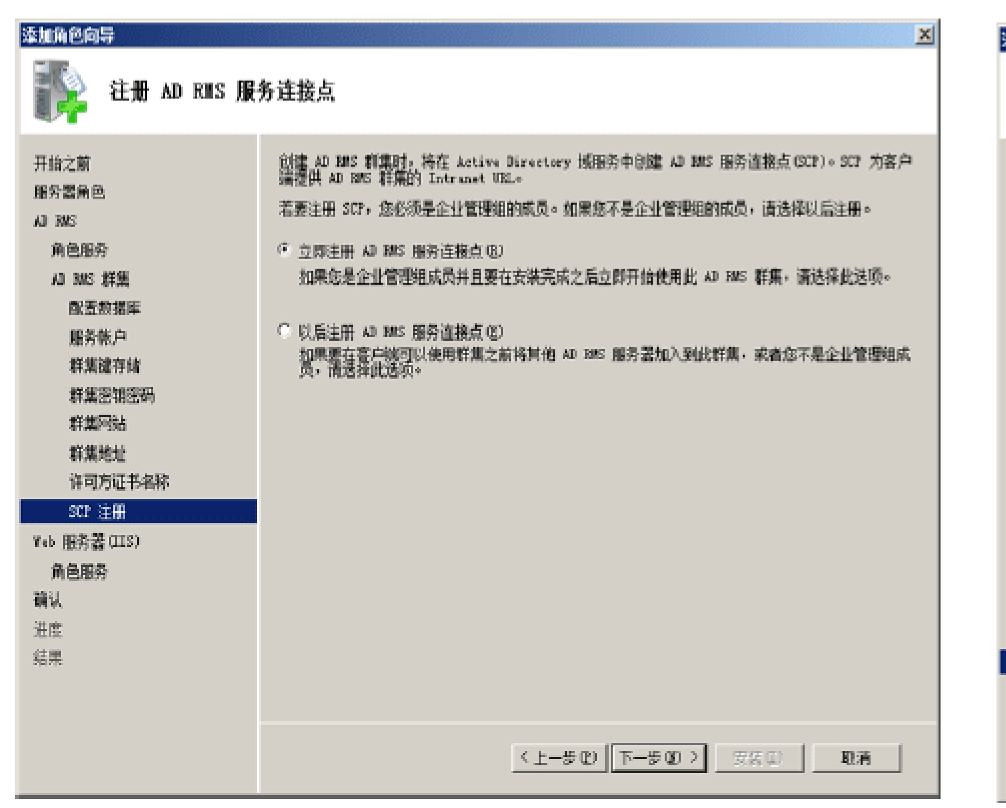




图 8.34　安装完成

08 单击“关闭”按钮，退出安装向导。根据提示信息，注销当前系统并重新登录。

8.3.3　配置 AD RMS 服务器

AD RMS 采用 MMC 控制台管理的方式，提供权限管理服务之前必须进行简单配置，如创建信任策略、权限模板等。选择“开始”→“管理工具”→“Active Directory Rights Management Services”命令，打开“AD RMS 控制台”窗口，如图 8.35 所示。如果选择 SSL 加密连接的方式，则在此过程中可能会出现“安全警报”提示框，直接单击“是”按钮跳过即可。

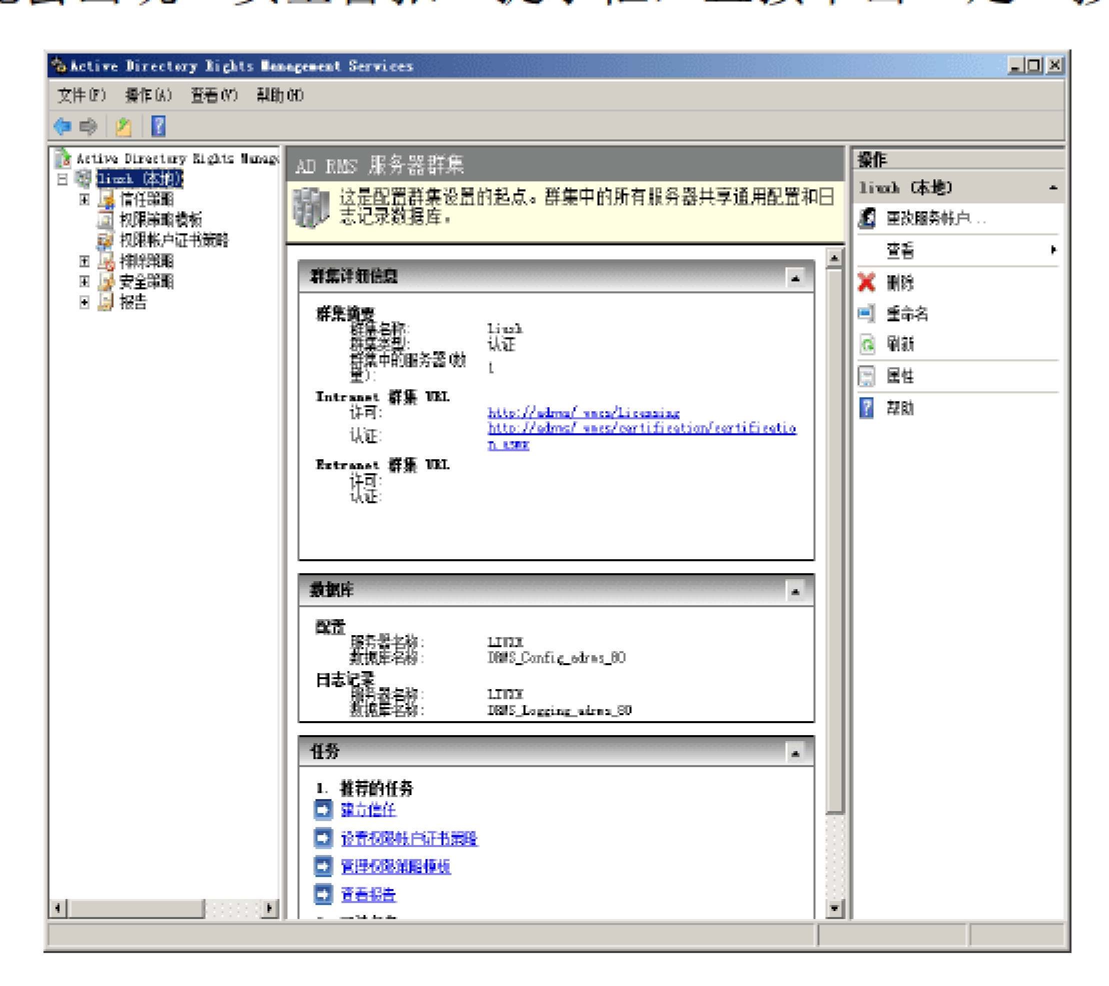


图 8.35　AD RMS 控制台

1. 配置信任策略

信任策略是不同 AD RMS 群集或不同域林中的 AD RMS 服务器之间建立信任关系的唯一标准，主要包括“受信任的用户域”和“受信任的发布域”。

（1）受信任的用户域

默认情况下，只有受信任的用户域才可以使用当前 AD RMS 服务器提供的权限保护服务，

不同 AD RMS 群集或不同林中的 RMS 服务器都是通过彼此的许可证书来识别的。用户可以通过将其他 AD RMS 群集中的信任用户域导出并添加至本地服务器中，来实现对其他用户提供权限管理服务。导出的信任用户域文件中会包括原 AD RMS 服务器的许可证信息，因此建立信任关系后，来自该域的用户就可以使用当前 AD RMS 服务器提供的使用许可证。

01 在 AD RMS 控制台窗口中，依次选择“信任策略”→“受信任的用户域”命令，显示如图 8.36 所示“受信任的用户域”窗口。在“受信任的用户域信息”列表中默认显示的是本地用户域，右击并选择快捷菜单中的“属性”命令即可查看其详细信息。

02 在右侧的“操作”栏中，单击“导入受信任的用户域”链接，在“受信任的用户域文件”文本框中输入文件的保存路径，或单击“浏览”按钮选择；在“显示名称”文本框中，输入该用户将在列表中显示的名称，用来进行标识。

03 单击“完成”按钮，即可完成用于域的添加。重复操作，可添加多个受信任的用户域。

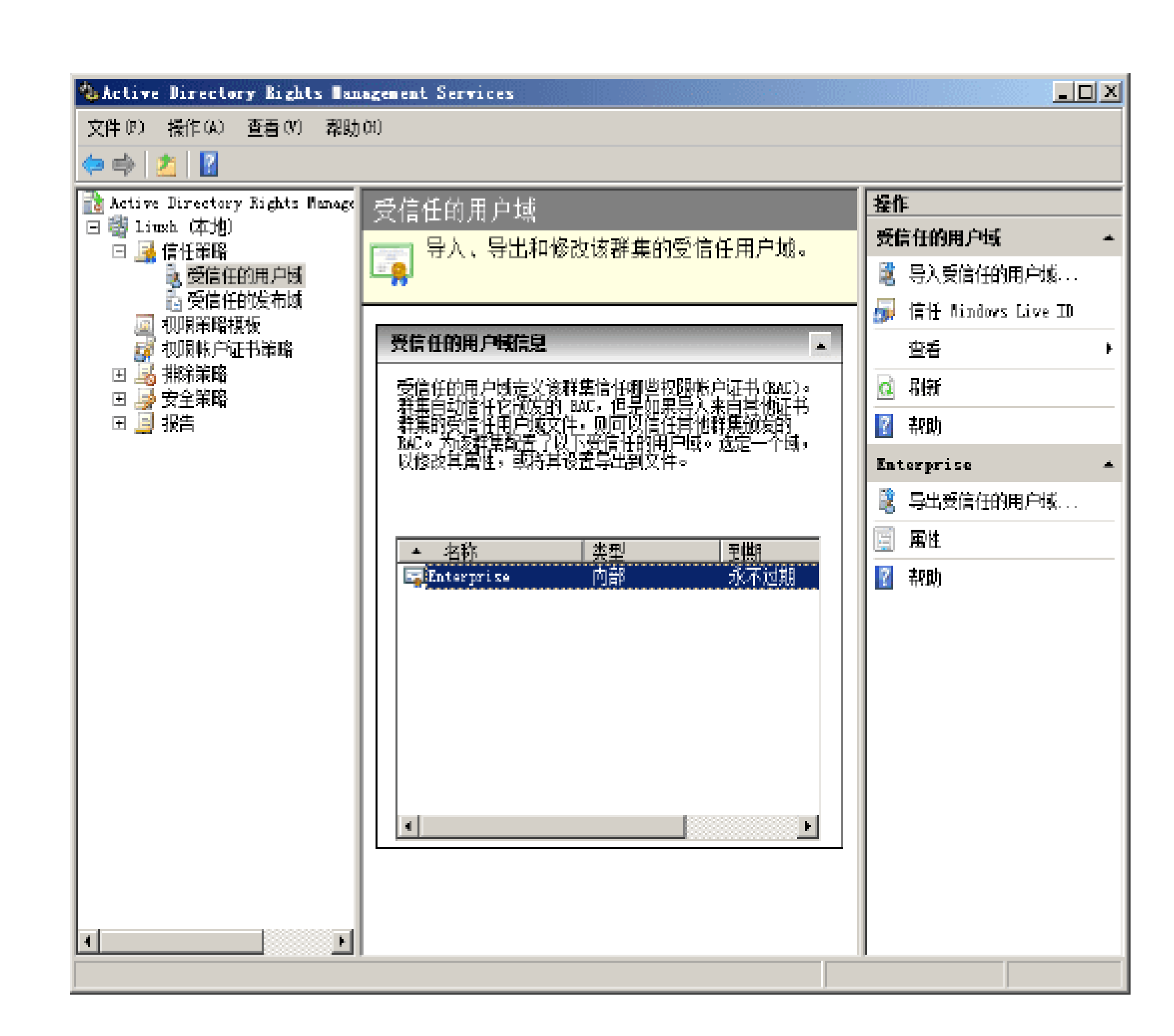


图 8.36　受信任的用户域



注意　在“受信任的用户域信息”列表中，右击域选项，在弹出的快捷菜单中选择“导出受信任的用户域”命令，还可以将其导出，以备本地恢复使用，也可以导入到其他 AD RMS 群集中，用于接受其他 AD RMS 服务器的权限许可证。

（2）受信任的发布域

在 AD RMS 控制台窗口中，单击“受信任的发布域”显示如图 8.37 所示“受信任的发布域”窗口。

受信任的发布域用于定义哪些 AD RMS 群集发布的许可证受到此群集的信任，与受信任的用户域恰恰相反，列表中默认存在的是本地服务器的记录。受信任的发布域文件的导出和导入与受信任的用户域文件类似，不同的是发布域文件的类型为.XML，其中包括将要信任的 AD RMS 服务器许可方证书、群集密钥和模板等信息。另外，发布域文件本身是受密码保护的，导入时必须输入原 AD RMS 服务器上使用的存储密码。

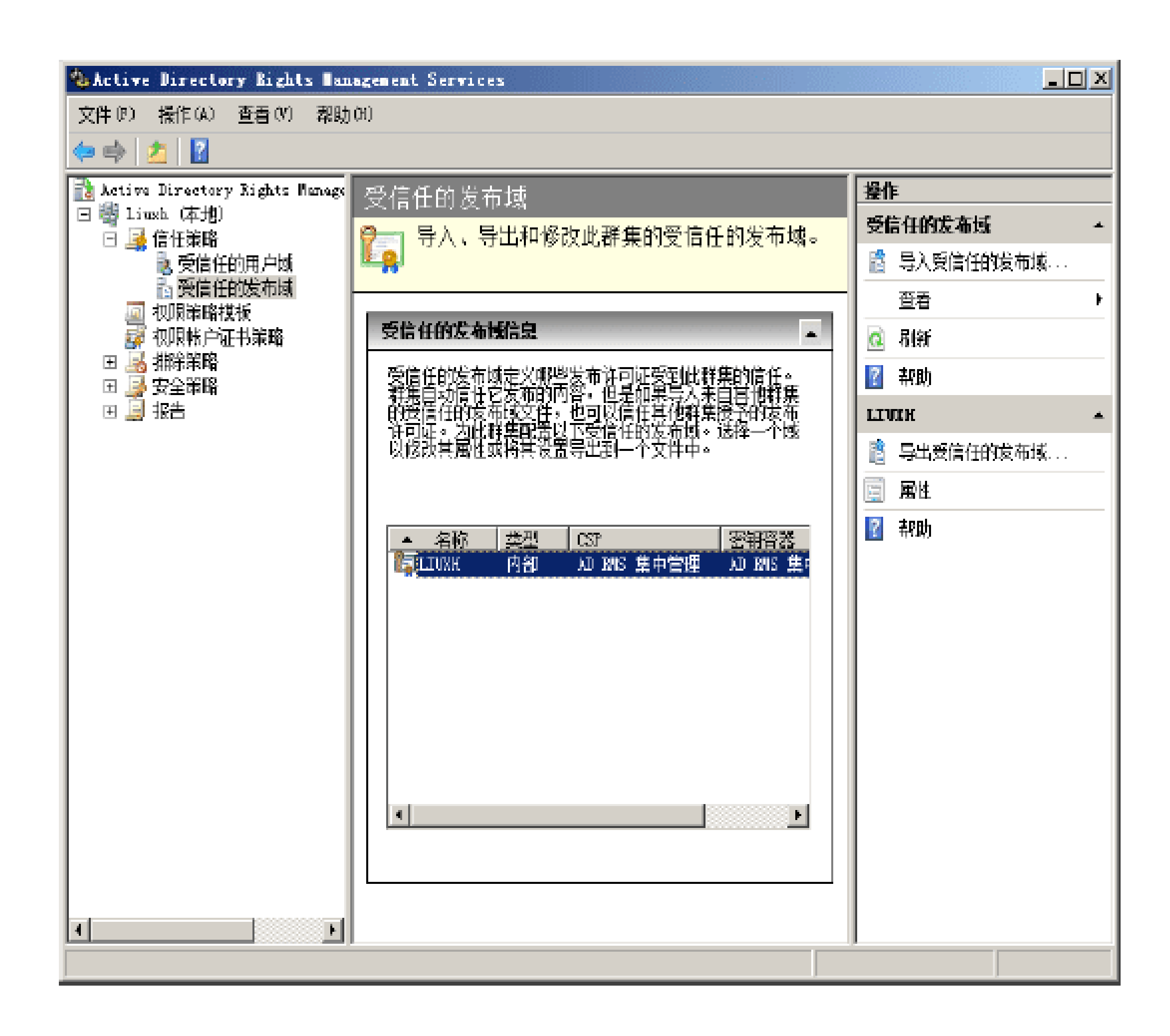


图 8.37　受信任的发布域

2. 配置权限策略模板

（1） 创建权限策略模板

机密程度不同的文档发布到客户端后设置的权限也有所不同，此时需要为该文档应用不同级别权限的策略模板。权限策略模板是为定义用户的权限策略用的，管理员可以通过定制一些现成的策略模板让企业用户直接调用。

01 在“AD RMS 控制台”窗口中，单击“权限策略模板”显示如图 8.38 所示“分布式权限策略模板”窗口。

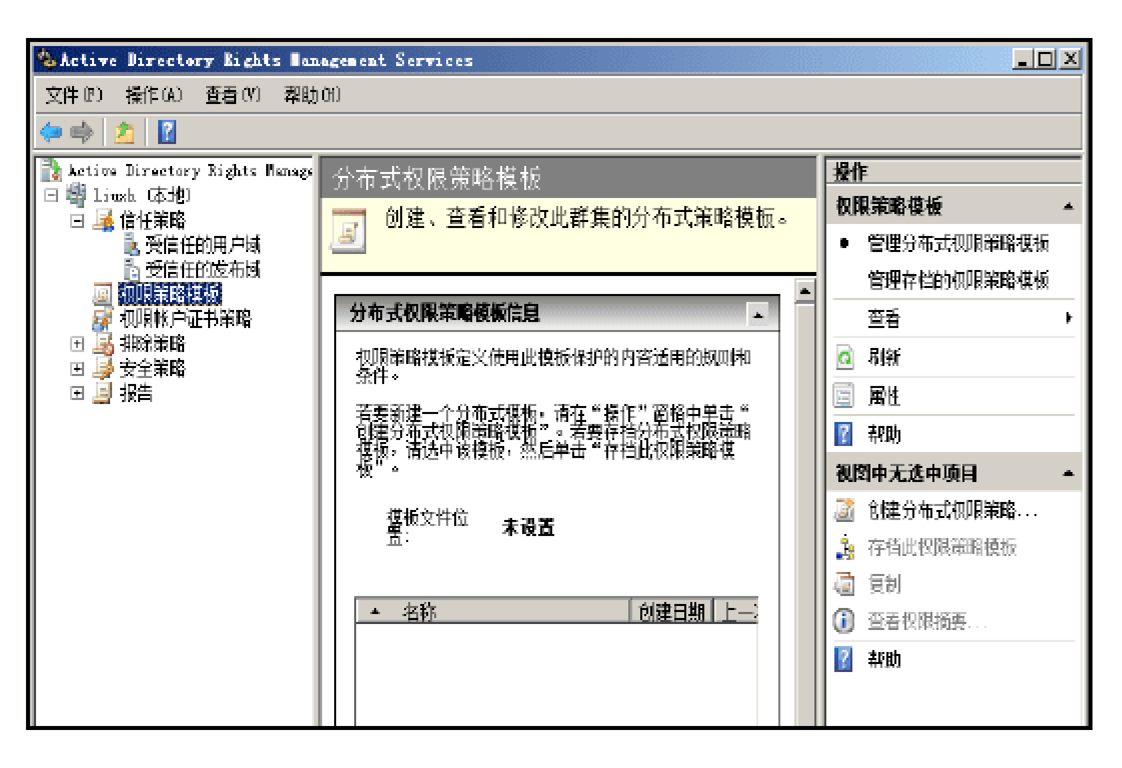


图 8.38　分布式权限策略模板

02 单击“操作”栏中的“创建分布式权限策略模板”链接，启动创建向导，在“添加模板标识信息”对话框中，单击“添加”按钮，显示如图 8.39 所示“添加新的模板标识信息”对话框。在“名称”文本框中输入新建模板的名称，“描述”文本框中输入相关描述信息。单击“添加”按钮，将其添加至“模板标识”列表中。

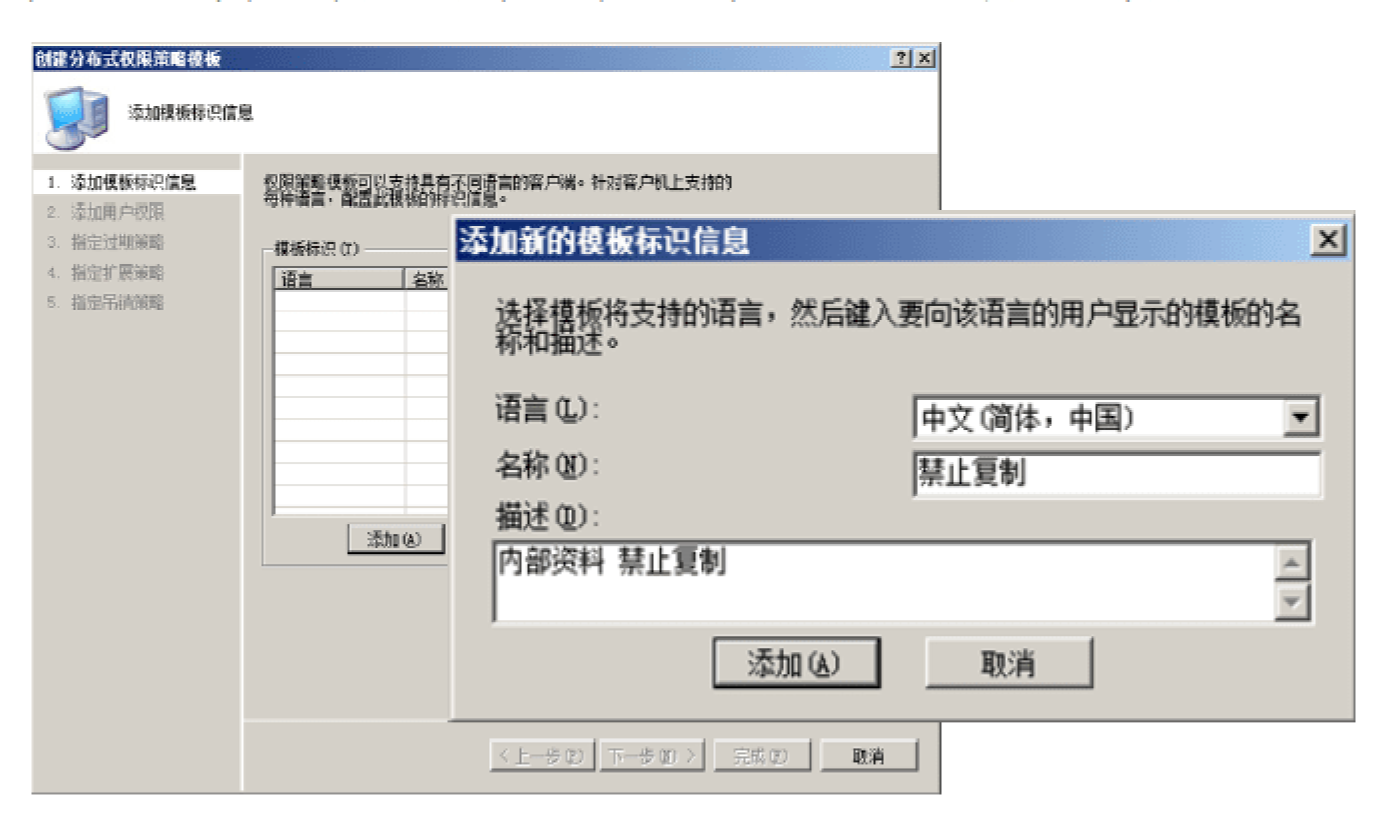


图 8.39　“添加新的模板标识信息”对话框

提示　“语言”文本框是专为使用不同语言的客户端设置的，如果客户端只支持英文显示，则可以在“添加模板标识信息”对话框中再次单击“添加”按钮，并选择“英文”语言即可。需要注意的是，要想使选择的语言生效，必须先在服务器上安装该语言。

03 单击“下一步”按钮，显示如图 8.40 所示“添加用户权限”对话框，默认情况下“用户和权限”列表是空的，即只选中“授予所有者不会过期的完全控制权限”复选框，其他用户帐户没有任何权限。单击“添加”按钮，在“添加用户或组”对话框中，选择“用户或组的电子邮件地址”单选按钮，即可在下面的文本框中输入用户对应电子邮件地址，也可以单击“浏览”按钮，打开“选择用户或组”对话框，

直接从当前域控制器中查找添加。如果选择“任何人”单选按钮，对当前域中的所有用户帐户有效。

图 8.40　添加用户权限



注意　如果要添加用户，应事先在域控制器上，打开用户属性对话框，为用户添加电子邮件地址。同样，如果要添加用户组，也要打开用户组属性，添加电子邮件地址。

04 单击“确定”按钮，将所选用户添加至列表中。重复操作，可添加多个用户或组的电子邮件地址。然后，在“用户和权限”列表中，选择赋予用户的权限，例如，要求做到“禁止复制”，只选中“查看权限”复选框即可。



注意　权限列表中给出的所有权限都是允许的，即只要选择某项，就表示要赋予用户相应的权限。如果模板赋予用户的权限无法完成相应工作，或在模板权限规定的时间和日期内没有完成工作，则可以通过“权限请求 URL”选项，向管理员发出权限请求，以再次获得权限或附加权限。

05 单击“下一步”按钮，显示如图 8.41 所示“指定过期策略”对话框。在“内容有效期限”命令区域中，可以定义当前模板中的权限信息何时过期或有效期限等，默认为“永不过期”。内容过期后，如果仍需要使用该策略信息，必须重新发布一次。

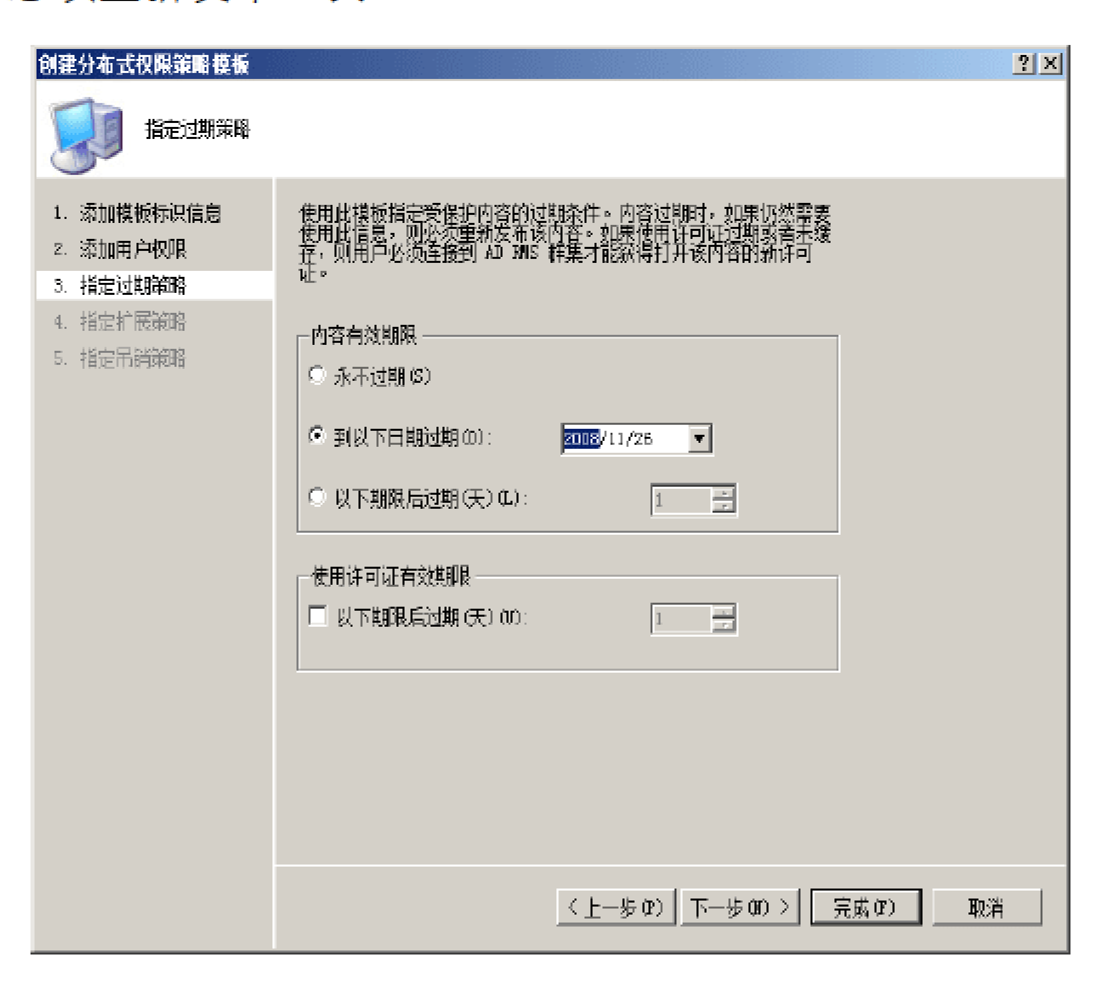


图 8.41　“指定过期策略”对话框

06 单击“下一步”按钮，显示如图 8.42 所示“指定扩展策略”对话框。

- “使用户能够使用浏览器加载项查看受保护的内容”：该项对于没有安装 Office 的客户端是非常实用的，只需安装相关插件即可在浏览器中查看受 RMS 保护的 Office 文档，建议选择该项；
- “每次使用内容时需要更新使用许可证（禁用客户端缓存）”：该项虽然可以使被保护文档更安全，但客户端每次使用时就会非常繁琐；
- “如果您要为其用 AD RMS 的应用程序指定其他信息，则可以在此处以名称-值对的形式指定”：选中该复选框，可在下面的列表中添加特定应用程序需要的名称和权限值，普通用户无需设置。

07 单击“下一步”按钮，显示如图 8.43 所示“指定吊销策略”对话框。吊销是 AD RMS 的一项重要功能，实施吊销之前必须先手动创建一个吊销列表，并为每个吊销列表生成一个公钥/私钥对，然后使用私钥签署吊销列表；另外，还必须为吊销列表指定一个用户可以访问的 URL 地址或 UNC 路径。通常情况下，不需要 AD RMS 服务器吊销，即不选择该复选框。



图 8.42 “指定扩展策略”对话框

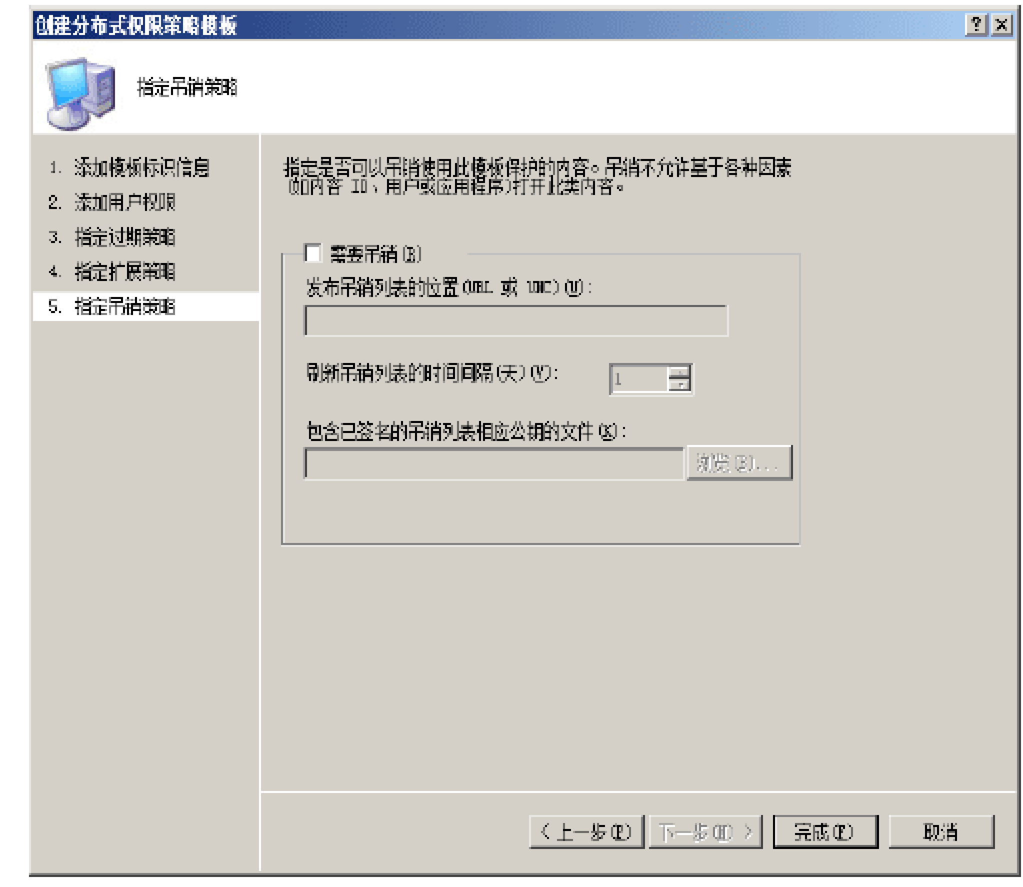


图 8.43 “指定吊销策略”对话框

08 单击“完成”按钮，退出创建向导，返回“权限策略模板”窗口。新创建的模板已经出现在列表中，此时虽然已经创建成功，但并不能立即应用。

09 右击新创建的策略模板，在弹出的快捷菜单中选择“存档此分布式权限策略模板”命令，将其本地存档，显示如图 8.44 所示“存档权限策略模板”对话框。提示一旦保存后，将不能再分发或导出该模板。单击“是”按钮保存即可。至此，新创建的权限策略模板才可以保存到本地模板库中备用。

10 返回“分布式权限策略模板”窗口，单击“管理存档的权限策略模板”链接，所有已存档的策略模板即可显示在“公布式权限策略模板”列表框中，管理员可以继续修改和查看其各项属性信息。如图 8.45 所示是新建策略模板的权限摘要。

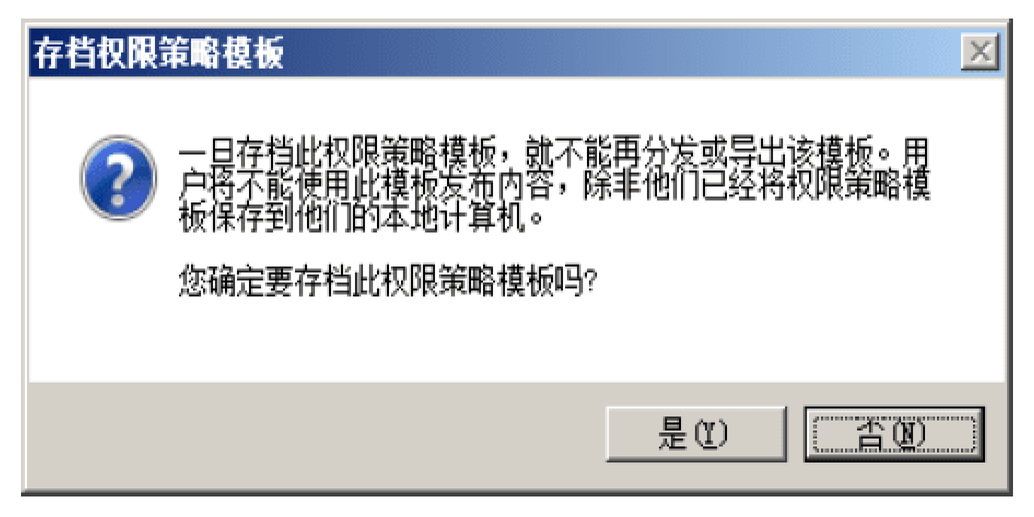


图 8.44　“存档权限策略模板”对话框

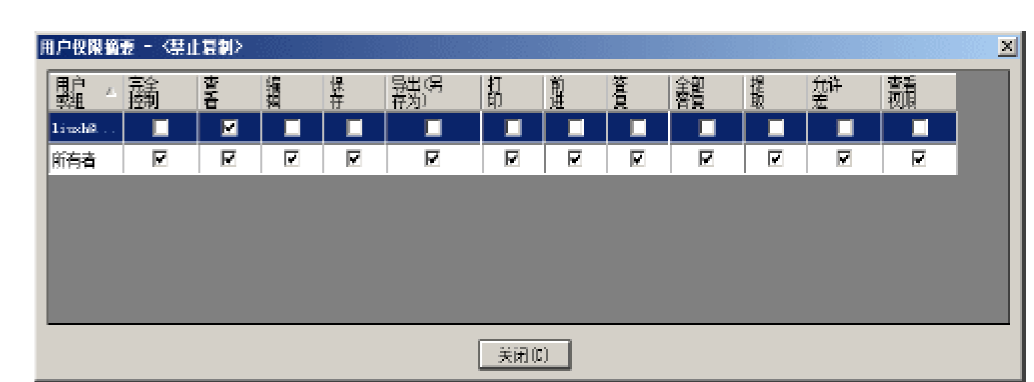


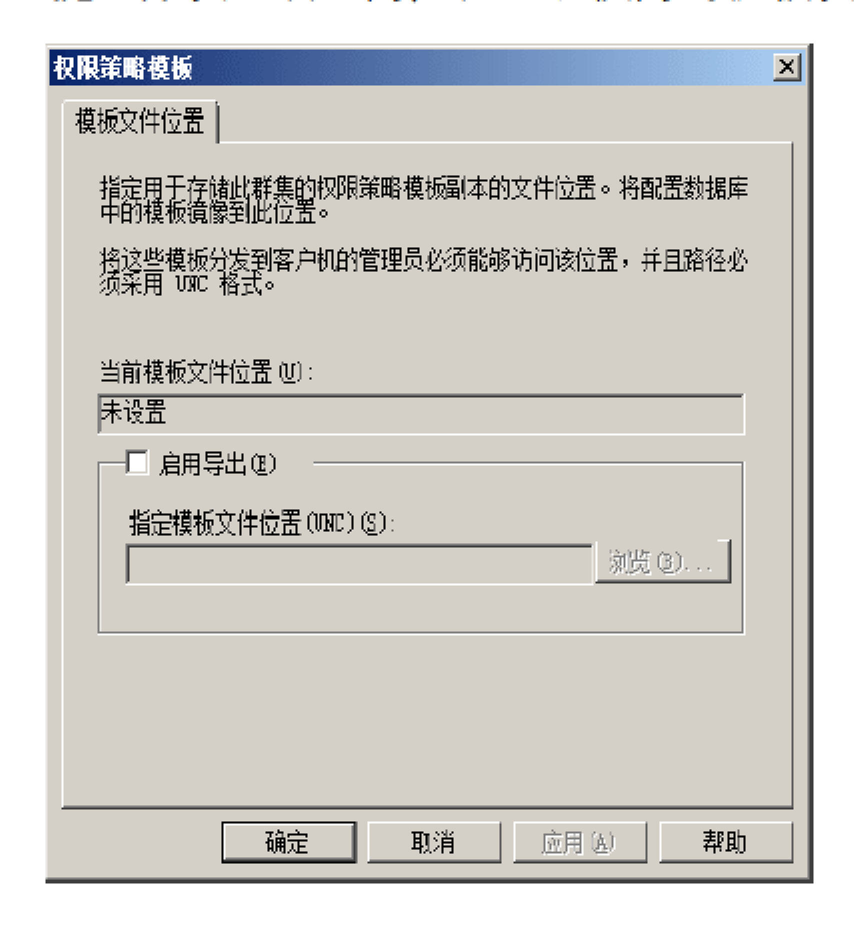
图 8.45　用户权限摘要

（2）　分发权限策略模板

客户端必须将服务器上创建的权限策略模板保存到本地计算机才可以使用，可以通过文件共享、网络传输、移动存储介质等方式获得。默认情况下，权限策略模板的保存位置为“未设置”。为了便于保存和用户使用，应在群集中指定一个公共文件夹，用于保存所有的策略模板。

01 在“权限策略模板”窗口中，单击“操作”栏中的“管理分布式策略模板”链接，在“分布式权限策略模板”窗口下方单击“更改分布式权限策略模板文件位置”链接，打开如图 8.46 所示“权限策略模板”对话框。选择“启用导出”复选框，在“指定模板文件位置”文本框中输入已经设置好的共享文件夹路径。注意，这里必须使用 UNC 格式，并且确定已经为指定用户帐户赋予了写入权限。

02 设置完成后单击“确定”按钮。然后，单击“管理存档权限策略模板”链接，选择想要分发的模板，右击并选择快捷菜单中的“分发此权限策略模板”命令，显示如图 8.47 所示“分发权限策略模板”对话框。提示分发之后，用户便可以使用此模板发布新内容。





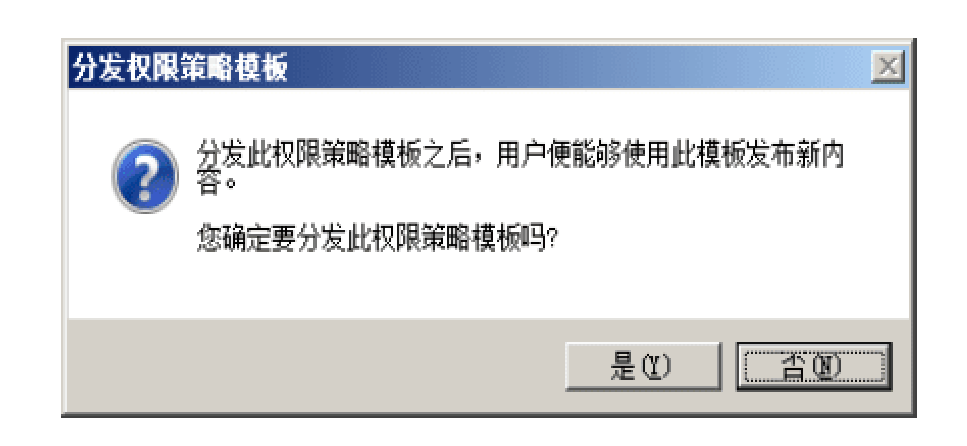


图 8.46　“权限策略模板”对话框　　　图 8.47　分发权限策略模板

03 单击“是”按钮确认即可。

注意　如果模板是从另一台 RMS 服务器迁移到此 RMS 服务器，在使用该模板之前，必须由此服务器签署，然后重新分发到客户端。

（3）　撤销权限策略模板

当某个权限策略模板不再适用时，可以将其删除。删除权限策略模板时，同时应删除用户计算机上的该模板，以便用户试图使用由已撤销的权限策略模板发布的内容时不会出现问题。当作

者使用权限策略模板发布内容时，该发布请求将被发送到 RMS 服务器。RMS 将使用数据库中存储的该权限策略模板的副本来响应该请求。如果数据库中不存在该权限策略模板，请求将失败。

（4） 备份和恢复权限策略模板

要保护重要的权限策略模板，可以将配置数据库中的模板数据定期备份到媒体中，并将该媒体存放到安全的地方。这样，当系统发生故障时，管理员就可以使用备份的副本来恢复权限策略模板。

3. 配置权限帐户证书策略

权限帐户证书（RAC）是 AD RMS 服务器颁发给每个客户的认证凭证，该证书将用户帐户与一个受保护的密钥对关联，而密钥对则专用于用户的计算机。用户可以通过这些证书来发布和使用受 AD RMS 保护的内容。每个证书都包含一个公钥，以向用户授予使用相关信息的权限。

打开“AD RMS 控制台”窗口，在左侧栏中选择“权限帐户证书策略”命令，显示如图 8.48 所示“权限帐户证书策略”窗口。

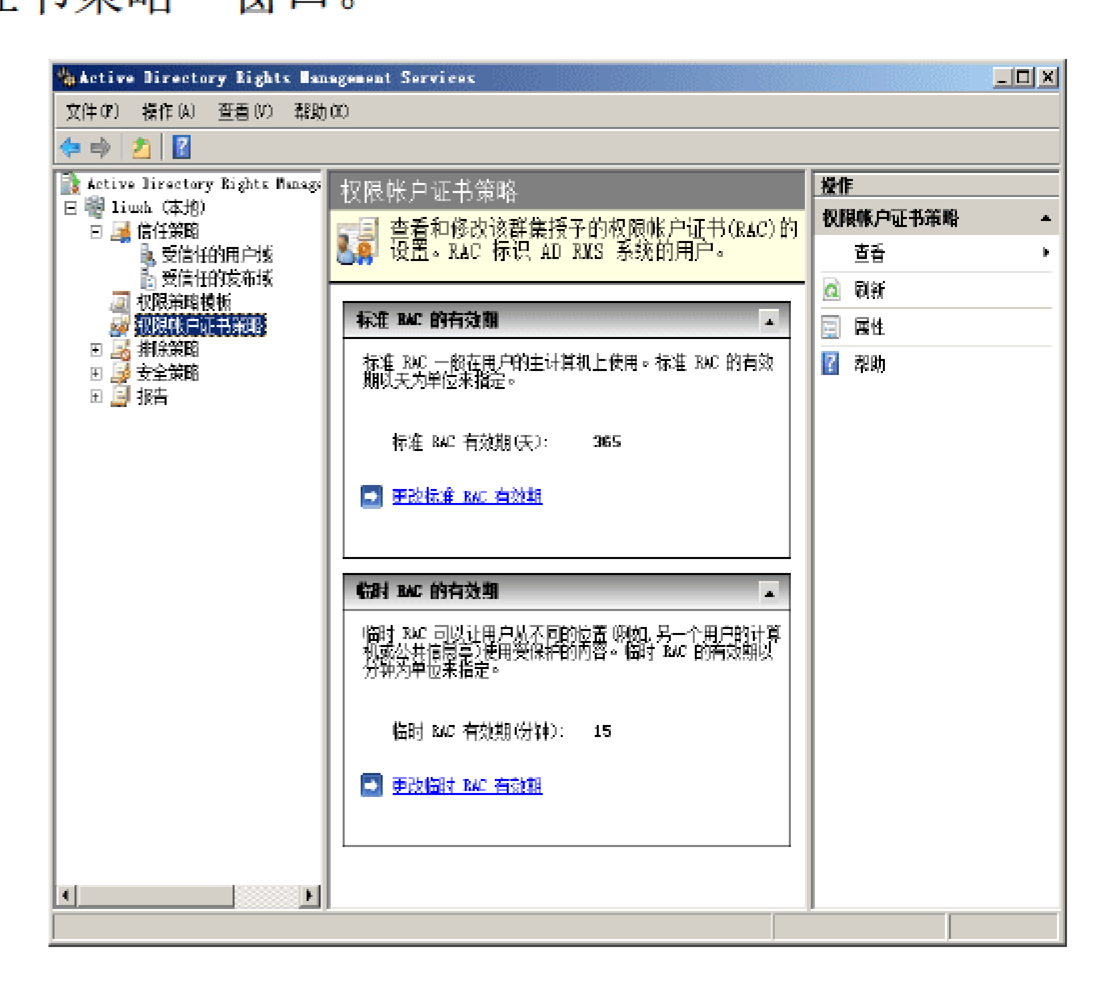


图 8.48 “权限帐户证书策略”窗口



提示 权限帐户证书根据有效期的长短和应用环境的不同，可分为标准 RAC 和临时 RAC。标准 RAC 的默认有效期限是 365 天，通常应用于固定用户的计算机上；临时 RAC 的默认有效期限为 15 分钟，主要是为了方便用户在不同位置都可以使用受 AD RMS 保护的文档。

权限帐户证书的有效期限可以根据实际需要更改。单击“更改标准 RAC 有效期”链接，显示如图 8.49 所示“权限帐户证书策略”对话框，在“标准 RAC 的有效期（天）”文本框中键入合适数值即可，有效期的范围是 1~9 999 天。

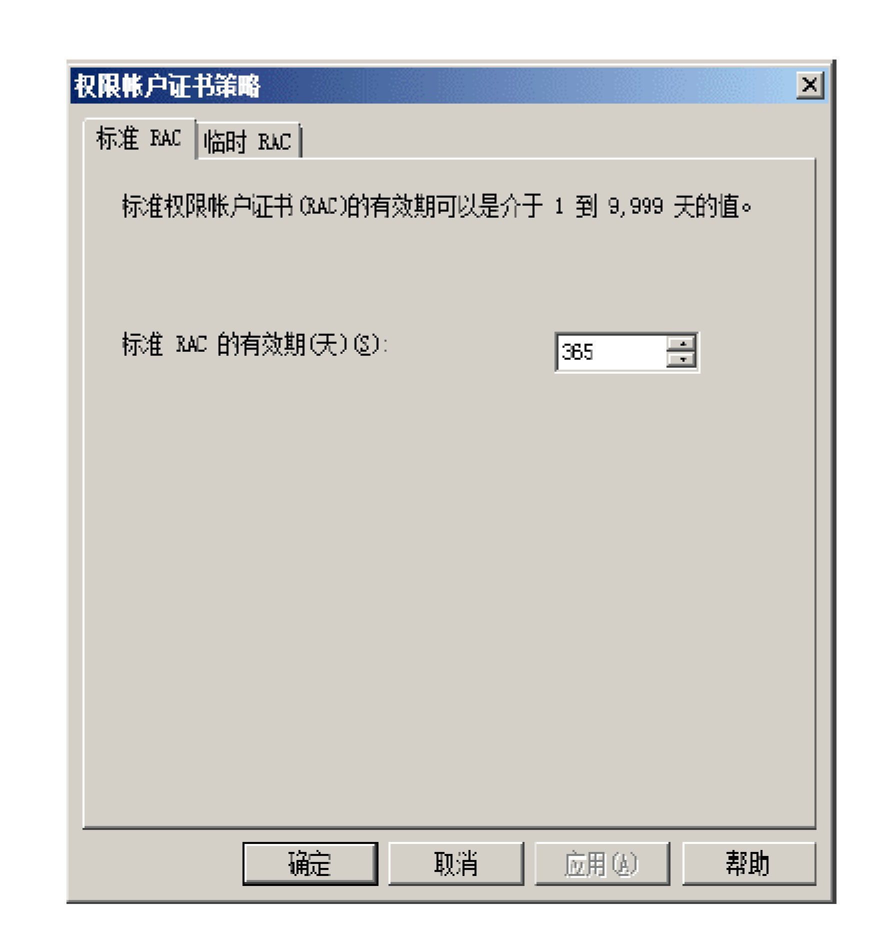
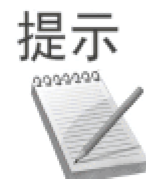


图 8.49　“权限帐户证书策略”对话框

8.3.4　AD RMS 客户端部署及应用

AD RMS 服务安装并配置完成以后，即可将需要接受 AD RMS 管理的客户端加入域，并部署 AD RMS 客户端。在 Windows Vista 系统中，RMS 客户端的名称已更改为 Active Directory 权限管理服务（AD RMS）客户端，并且已集成到操作系统中，因此不需要独立的安装。在早于 Windows Vista 的 Windows 操作系统版本中，RMS 客户端组件仍需要独立下载和安装。目前最新版本为 SP2 简体中文版下载地址为：

http://www.microsoft.com/downloads/details.aspx?displaylang=zh-cn&FamilyID=02da5107-2919-414b-a5a3-3102c7447838



提示　管理员还可以通过组策略、SMS、SCCM 等方式来向客户端统一分发客户端安装程序。如果客户端数量较少，则可以通过手动安装的方式实现。

1. 在 Windows 2000/XP 系统中安装 RMS 客户端

AD RMS 客户端安装过程非常简单，此处不做详细介绍。需要注意的是，更换登录的域用户帐户后，应重新运行客户端安装向导，并选择“修复带 Service Pack 2 的 Windows Rights Management 客户端”单选按钮。客户端需要将服务器上创建并保存的权限策略模板拷贝到自己的计算机上才可以使用，另外还需要在注册表中做相应修改。

01 通过网络共享或移动存储设备，将 AD RMS 服务器上存储的权限策略模板，复制到本地计算机上，如图 8.50 所示。

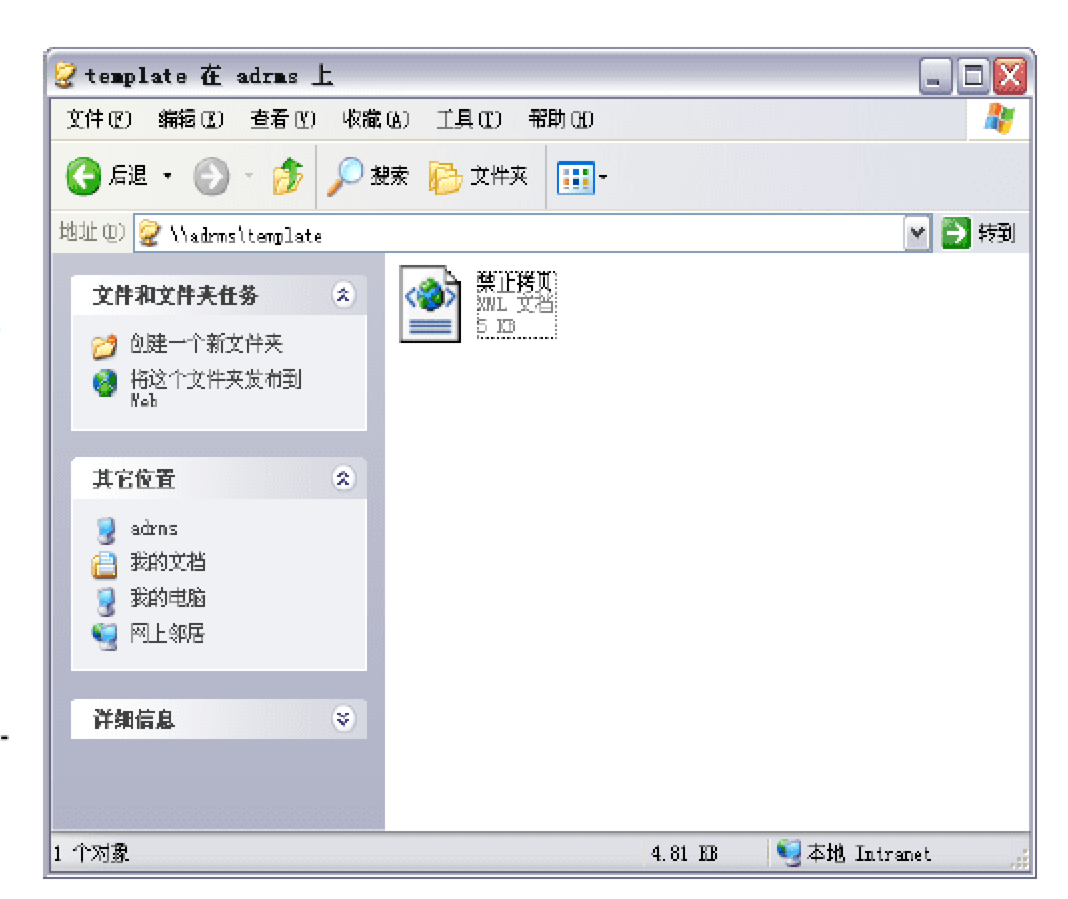


图 8.50　获取权限策略模板

02 打开注册表编辑器，并依次展开如下分支：

HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Common\DRM

在右侧窗口空白处单击鼠标右键，依次选择“新建”→“字符串值”，新建一个字符串值项目（如图 8.51 所示）。

03 将新创建的字符串值命名为“AdminTemplatePath”，然后双击该对象显示如图 8.52 所示“编辑字符串”对话框，指定该对象的数值数据为本地计算机上保存要应用的权限策略模板的路径。这里，将要保存在 E 盘根目录下，因此，输入“e:\”即可。

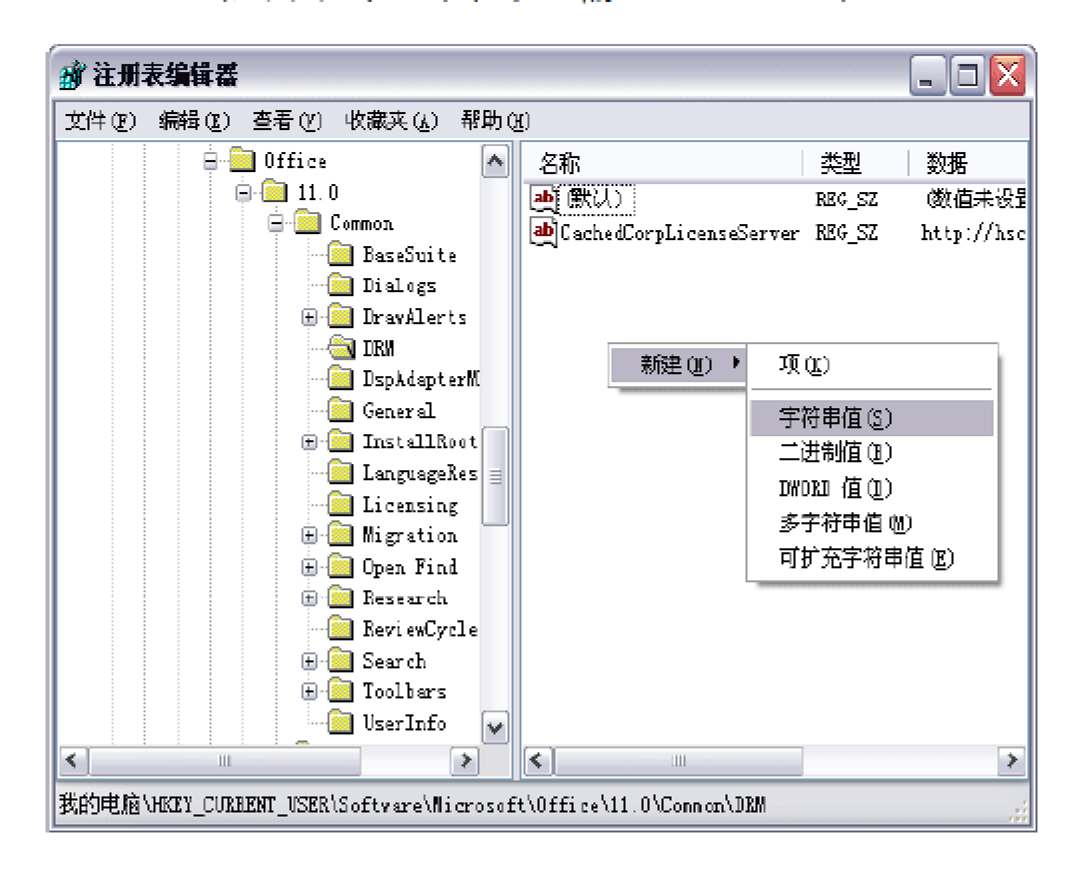


图 8.51　创建字符串值对象

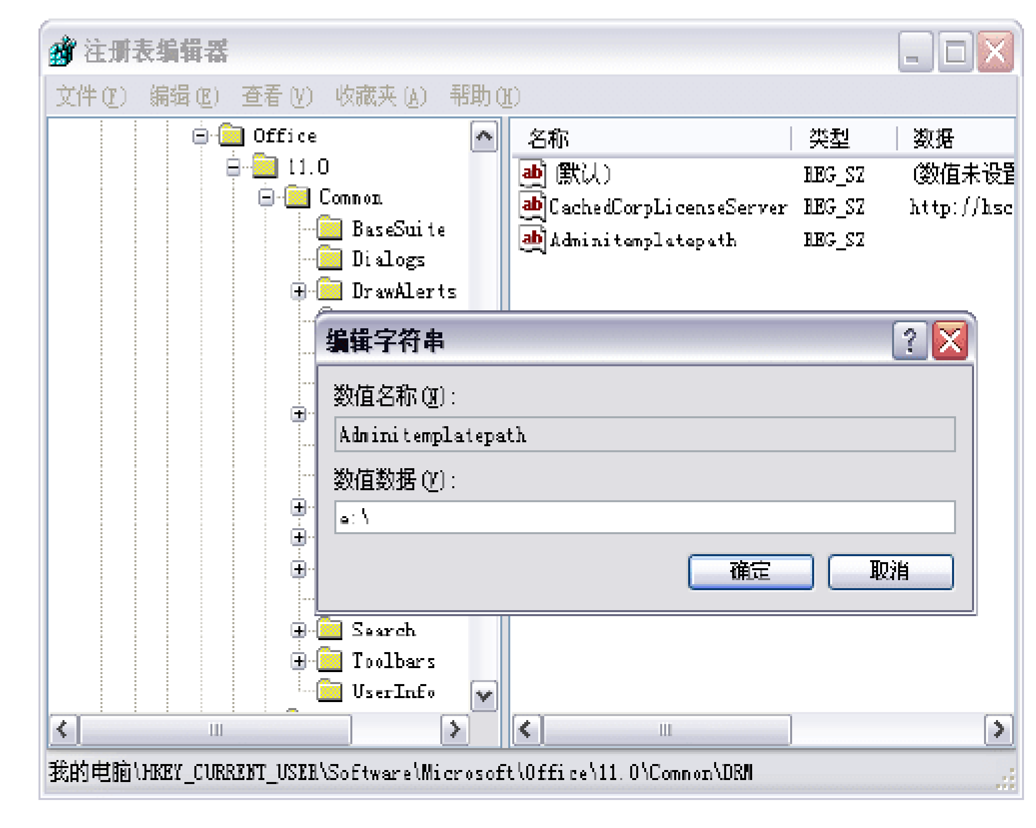


图 8.52　编辑字符串值

04 单击“确定”按钮保存设置并关闭注册表编辑器窗口。打开欲应用此策略模板的受保护文档，打开“文件”菜单中的“权限”选项，此时，会发现级联菜单中多出了一个可选项，即“禁止拷贝”，如图 8.53 所示。

05 选定相应策略模板后，共享工作区中会显示如图 8.54 所示“受限权限”等信息。授权人信息默认是本地登录帐户，当然管理员也可以在建立到服务器的连接时指定为其他用户，或直接单击“更改用户”链接随时更改。本例是 lhn@coolpen.net（所用模板针对的用户为 tjl@coolpen.net）。

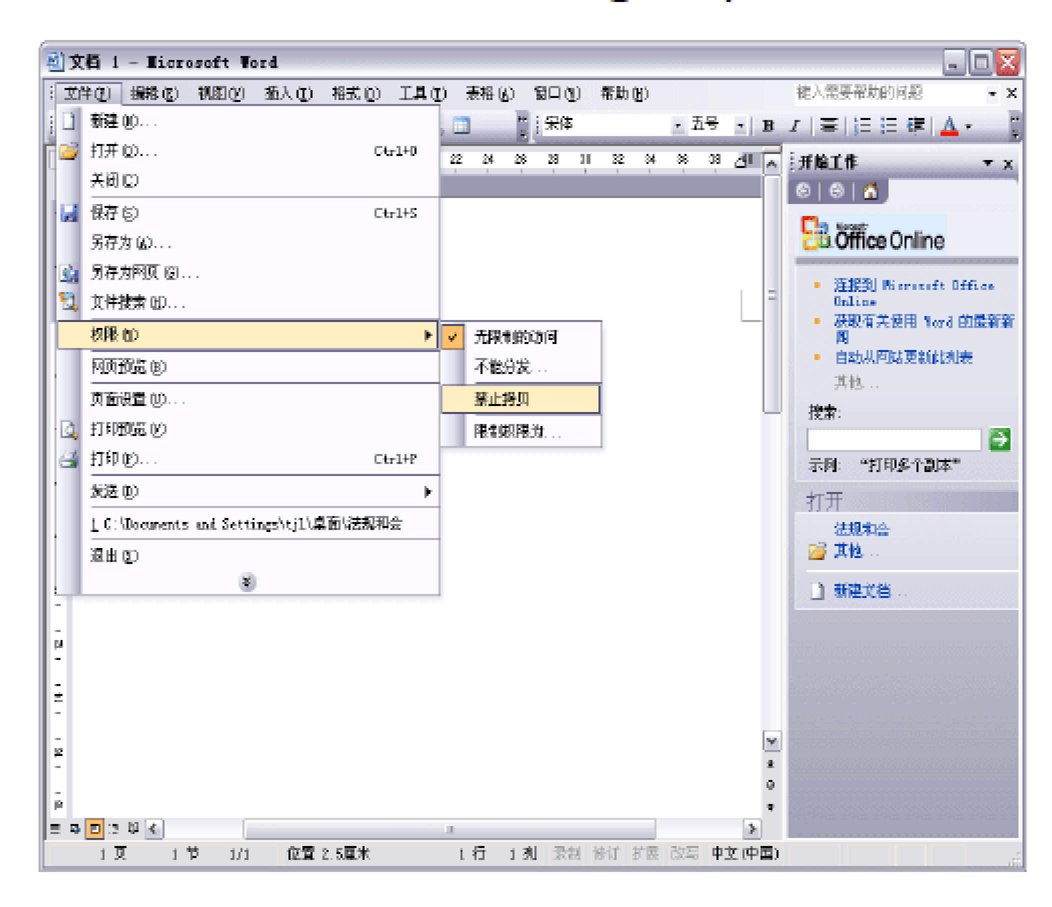
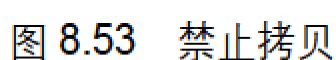



图 8.53　禁止拷贝

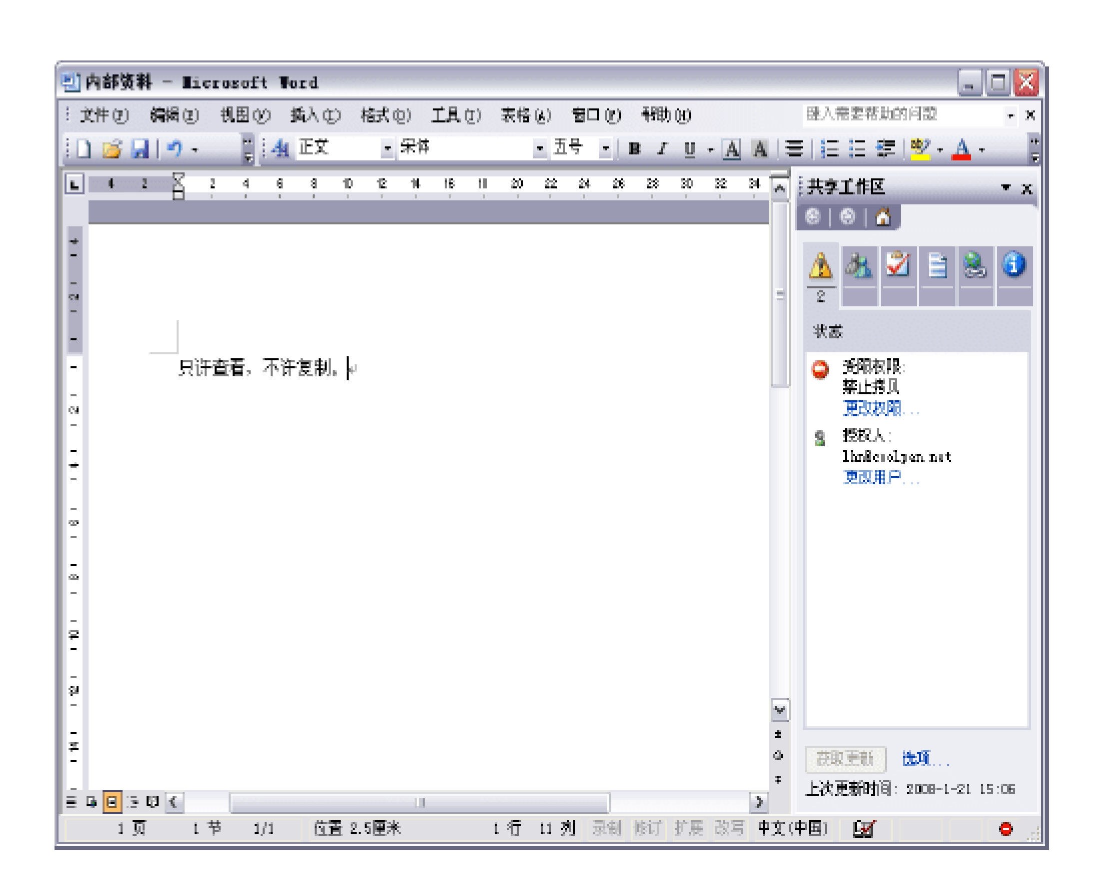


图 8.54　成功应用权限策略模板

06 单击共享工作区中的“更改权限”链接，可以查看当前用户帐户对该文档拥有的控制权限，显示如图 8.55 所示对话框。由于目前登录用户是该文档的创建者，在 RMS 配置该权限策略模板时，为文档作者赋予了完全控制的权限，即所有权限的状态都是“是”。

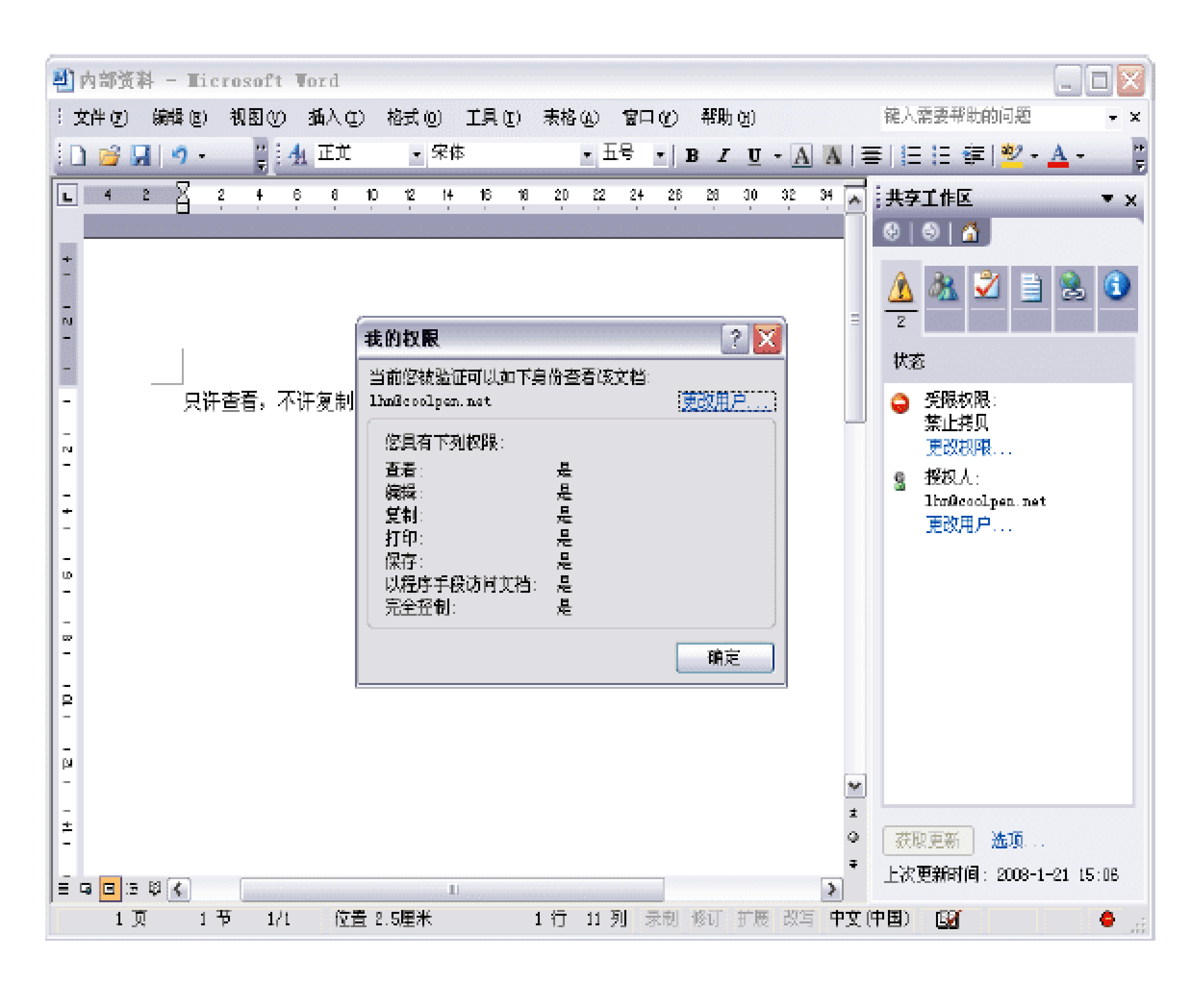


图 8.55　当前用户权限

2. 在 Windows Vista 系统中配置 AD RMS 客户端

Windows Vista 系统默认已经集成 AD RMS 客户端，用户只需进行相应配置即可使用。在 Windows 2000/XP 系统中安装 RMS 客户端之后，同样需要进行如下配置，这里以 Windows Vista 系统中的 Office Word 2007 为例加以介绍。

使用 AD RMS 服务器上策略模板中希望限制的域用户帐户登录客户端计算机，如图 8.56 所示。由于该用户帐户需要在本地计算机上保存策略模板，所以必须拥有对目标文件夹的写入权限。

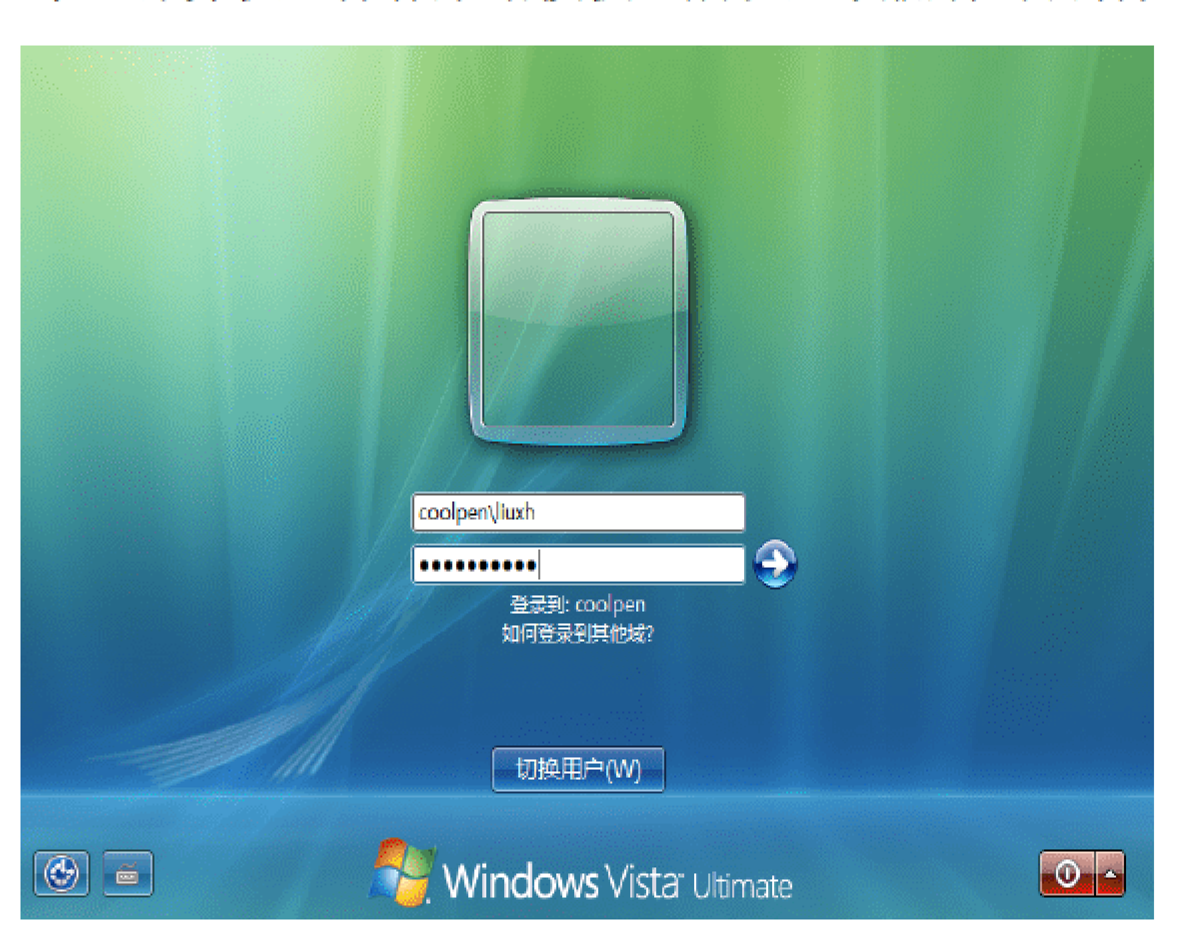


图 8.56　登录到客户端



注意　默认情况，当前登录的域用户帐户将自动被添加到本地的 Users 组中，因此只需确保该组具有足够的操作权限即可。

通过网络共享或移动存储设备，将 AD RMS 服务器上存储的权限策略模板，复制到本地计算机上，并在注册表中修改相应键值，与 Windows XP 系统完全相同，此处不复赘述。应用过程也比较简单，打开欲应用此策略模板的受保护文档（以 Office Word 2007 为例），单击“Office 按钮”并依次选择“准备”→“限制权限”选项，此时，会发现级联菜单中多出了一个可选项，即“禁止复制”，如图 8.57 所示。

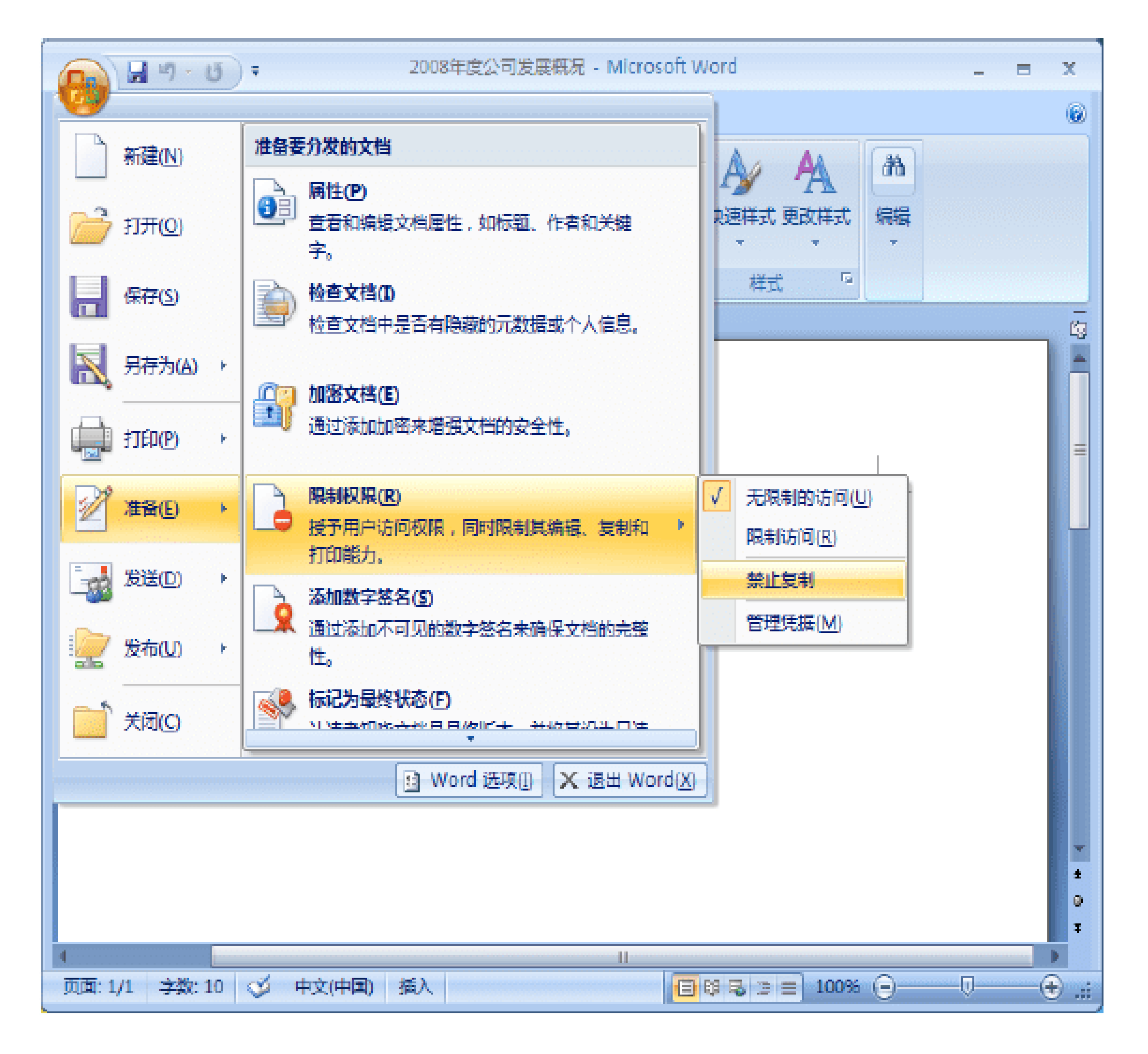


图 8.57　限制权限

3. 受限客户端应用被保护文档

AD RMS 策略模板主要是为了限制某些客户端针对文档享有的权限，因此当这些受限客户端应用被保护文档时，必须连接到 AD RMS 服务器进行凭据验证，并下载相应权限许可证才可以打开。这里，仍以上述应用为例进行介绍。

01 当用户 lhn@coolpen.net 创建好的文档，应用了限制用户 tjl@coolpen.net 复制和更改的权限，当用户 tjl@coolpen.net 拿到文档并查看时，会显示如图 8.58 所示提示框。

02 单击“确定”按钮，客户端开始向 AD RMS 服务器提交身份验证，并获得相应的权限，最终打开文档，显示如图 8.59 所示窗口。不过此时，文档是“只读”状态，并且不允许用户执行“复制”命令，或按下 PrtScrn 键抓取屏幕，这是因为当前被保护文档应用的权限策略模板已经屏蔽了 Windows 的这些功能，关闭受保护文档则一切恢复正常，用户使用时应注意。

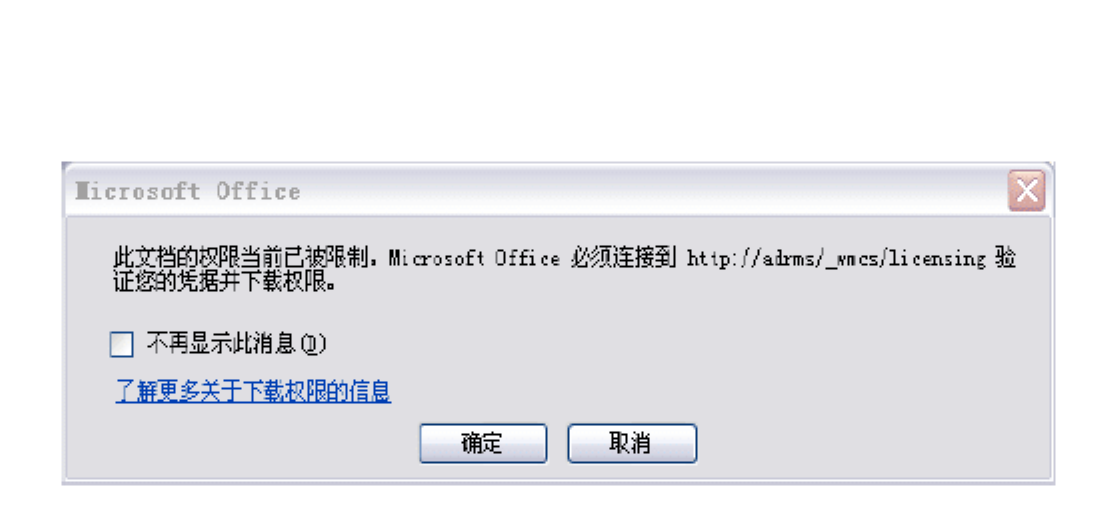


图 8.58　受限用户打开被保护文档

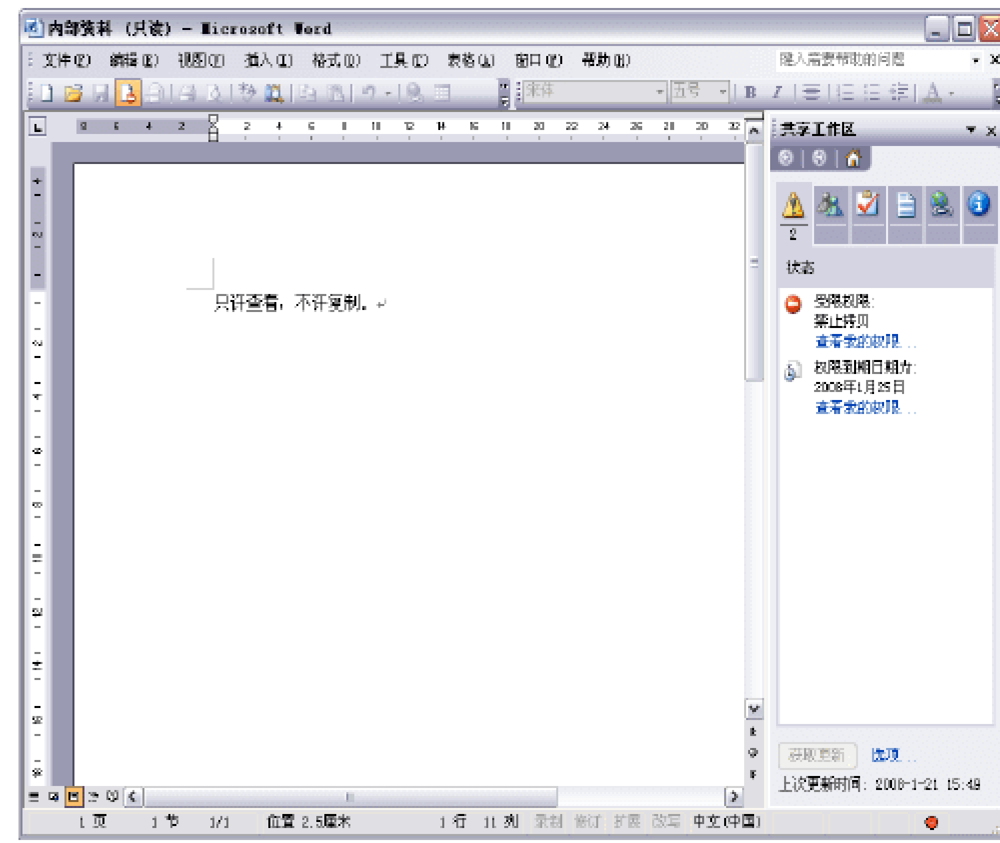


图 8.59　文档处于“只读”状态

03 单击“查看我的权限”链接，打开“我的权限”对话框，其中只有“查看”一项处于“是”状态，其他均为“否”。单击“更改用户”按钮，打开“选择服务”对话框，如果当前拥有的权限无法正常完成工

作，可以在这里选择其中一种方式添加其他有足够权限的用户帐户。选择“使用 Microsoft .NET Passport 帐户”单选按钮，可以凭借有效的 Microsoft .NET Passport 帐户从 Microsoft 获得一个证书，实现相应目的，这与 AD RMS 服务器的设置有关，如果添加了.NET Passport 类型的可信任用户域，客户端可以使用这种方式，否则无效。选择“使用 Microsoft Windows 帐户”单选按钮，即可从当前域中选择其他用户帐户来完成相应操作，如图 8.60 所示。

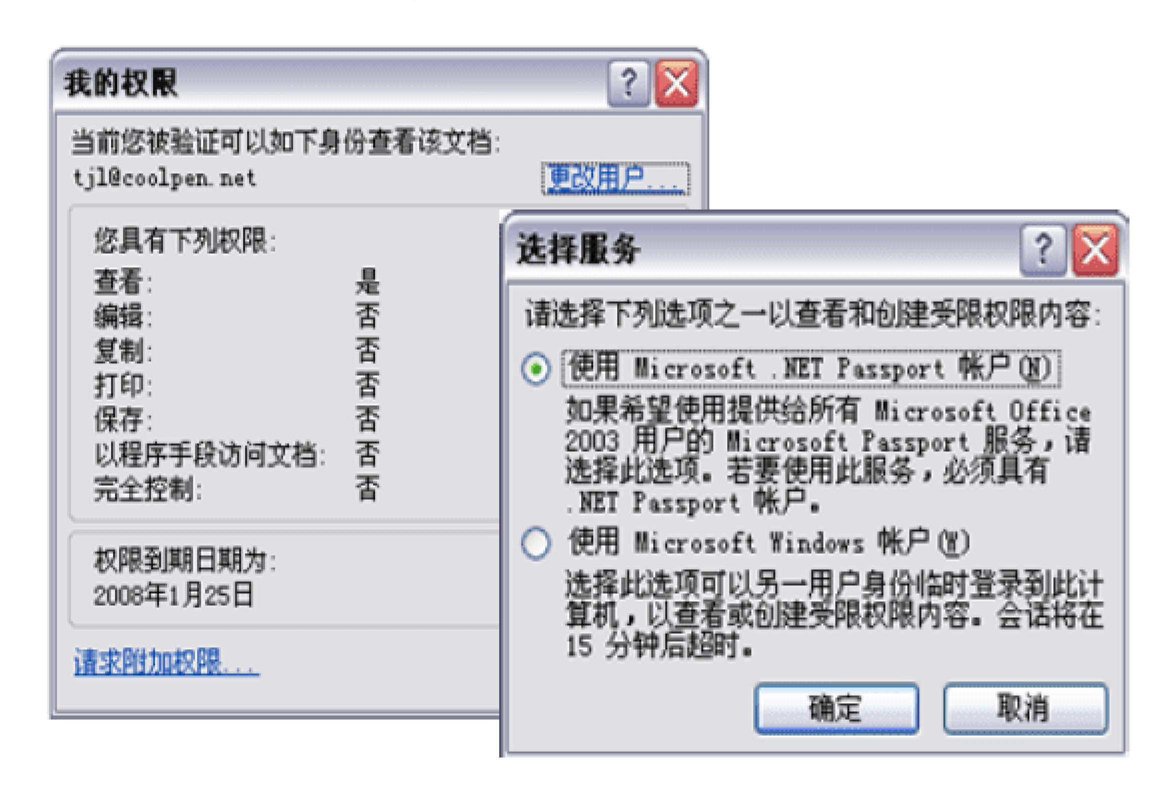


图 8.60　查看用户帐户权限

如果上述方法仍不能获得相应权限，可以在“我的权限”对话框中，单击“申请附加权限”连接，向 AD RMS 服务器申请相关权限，打开如图 8.61 所示窗口。“收件人”文本框中就是 AD RMS 服务器上设定的接收申请的电子邮件地址，保持默认即可。根据自己的实际需要，说明想要请求的权限即可。

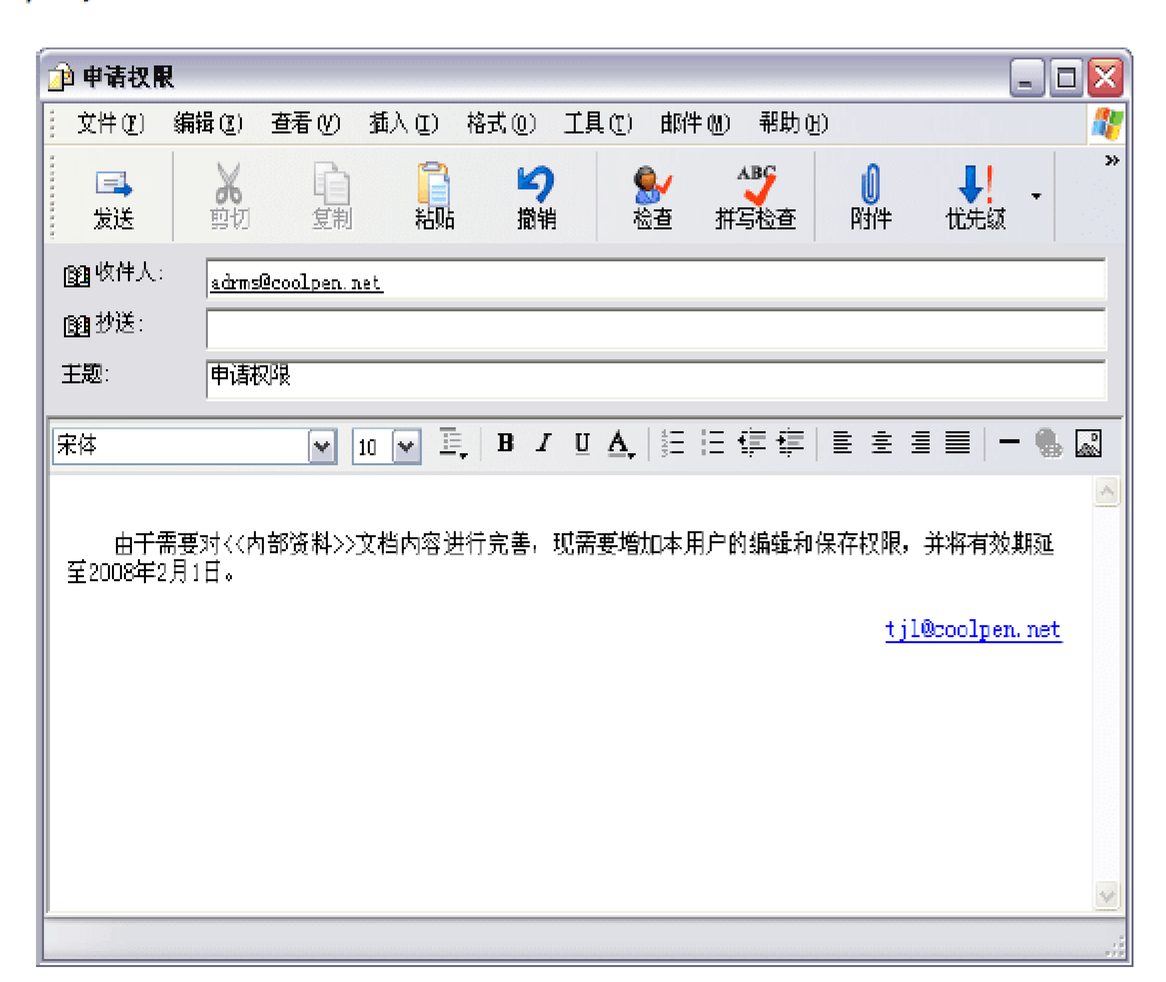


图 8.61　申请附加权限



提示　需要应用此功能时，必须先在网络中配置 Exchange 或其他邮件服务器。虽然在 AD RMS 系统中用到 E-mail 地址的地方非常多，但是多数情况下是作为一种用户标识，并非真正的用来传递信息，所以网络中邮件服务器也就可有可无。如果确实需要传递信息，则必须搭建邮件服务器。

小　　结

文件安全是一个广义的概念，包括文件存储安全和文件访问安全。本章介绍了当前最常用的文件安全保护技术，任何用户都可以轻松实现从创建到访问，从本机存储到网络共享的文件安全。随着用户文件安全要求的不断升级，在 Windows Server 2008 系统中集成了 AD RMS 服务器角色，管理员可以随时根据需要安装。AD RMS 服务器可以对需要保护的文档或程序提供全方位的安全防护，例如，禁止查看过程中转发和存储、设置文档的有效期限等。如果网络中没有部署 AD RMS 服务器，可以凭借有效地.NET Passport 帐户，登录到 Microsoft 提供的权限管理服务器，下载相关证书，实现对文档的保护。通常情况下，大多数用户都是通过共享权限保护共享资源的安全，其实最可取的方法是将 NTFS 权限和共享权限配合使用，有效控制网络用户对共享资源的访问。

习　　题

1. 对于文件安全，最基本的操作是哪些？
2. 创建共享文件夹的方法有几种？
3. 如何对共享的文件夹进行加密？
4. 如何对共享的文件夹进行管理？
5. 文件备份在文件安全中起着何种作用？

实验：配置共享资源安全

实验目的

掌握通过各种方法确保局域网共享资源的安全。

实验内容

创建共享资源，并通过 NTFS 权限、隐藏共享、共享权限等多种方式保护共享资源的访问安全。

实验步骤

1. 创建共享文件夹。
2. 设置 NTFS 访问权限。
3. 设置共享访问权限。
4. 将目标文件夹设置为隐藏共享。
5. 在网络中的其他计算机上访问共享资源。

第9章

服务器信息备份与还原

随着计算机网络应用的不断推广，局域网中的服务器角色也越来越丰富，当然网络管理员的工作负担也就相应增加中，要时刻确保这些服务器的正常运行。其中非常重要的一项工作就是备份服务器信息，以备不时之需。硬件设备故障、网络入侵等都可能造成数据丢失，甚至导致服务器死机。必要时，管理员可以使用先前做好的备份数据，快速还原业务应用，降低故障损失。

本章导读

- Active Directory 数据库的备份与还原
- DHCP 服务器的备份与还原
- DNS 服务器的备份与还原
- WINS 服务器的备份与还原
- 注册表的备份与还原
- 网络配置信息的备份与还原
- 磁盘配额的备份与还原

9.1　服务角色的备份与还原

服务角色是服务器上非常重要的信息之一。通常情况下，大部分服务角色的状态信息都是存储在独立的数据库中的，管理员只需将其备份出来，当需要重读服务器信息或遇到故障时，直接将备份信息导入即可。

9.1.1　Active Directory 数据库

Active Directory 数据库备份是管理员最重要的任务，建议管理员仔细规划 Active Directory 数据库备份策略。第一次备份时，建议完整备份整个系统，然后使用增量备份模式备份，安排备份计划自动完成 Active Directory 数据库的备份。在 Windows Server 2008 中备份 Active Directory 数据库，需要用到 Windows Server Backup 工具，安装和相关应用请参考本书“第 7 章 数据存储安全”中的相关介绍。

1. 完整备份 Active Directory 数据库

备份 Active Directory 数据库，可以使用图形模式，也可以使用命令行模式，此处以前者为例介绍。

01 打开“Windows Server Backup”窗口，单击“一次性备份”文字链接。打开“一次性备份向导”对话框，依次单击“下一步”按钮，设置备份选项、备份配置和备份项目，如图 9.1 所示。在“备份选项”对话框中，选择“不同选项”单选按钮。在“选择备份配置”对话框中，选择“整个服务器”单选按钮。在“选择备份项目”对话框中，选择需要备份的磁盘。



图 9.1　设置备份选项、备份配置和备份项目



02 依次单击“下一步”按钮，指定目标类型、保存路径和其他高级选项，如图 9.2 所示。在“选择备份目标”对话框中，选择用于存储备份的磁盘。在“指定高级选项”对话框中，选择要创建的备份类型。

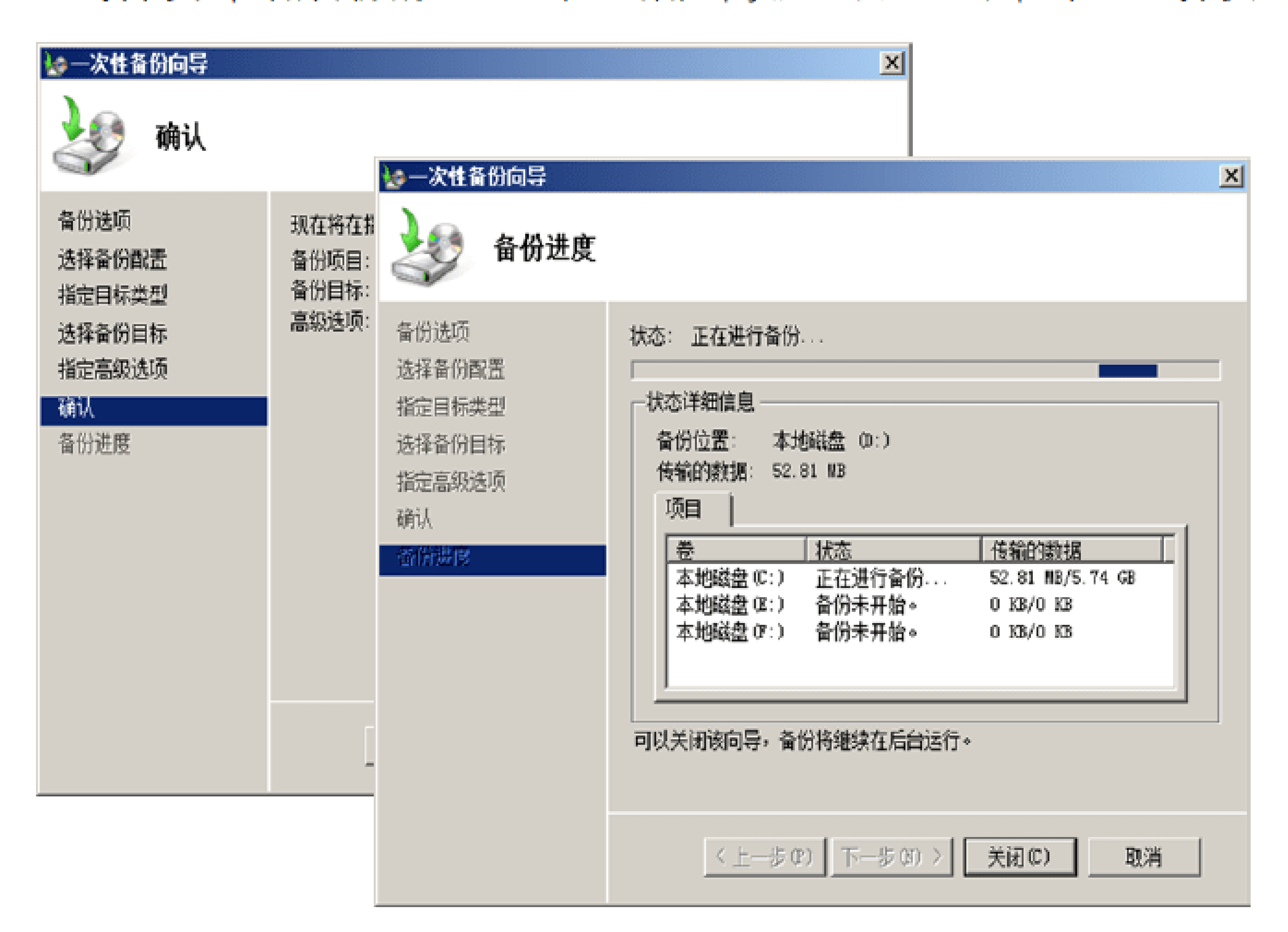


图 9.2　指定目标类型、保存路径和其他高级选项

03 单击“下一步”按钮，显示“确认”对话框，确认设置无误后单击“备份”按钮，即可开始备份，直至备份创建完成，如图 9.3 所示。

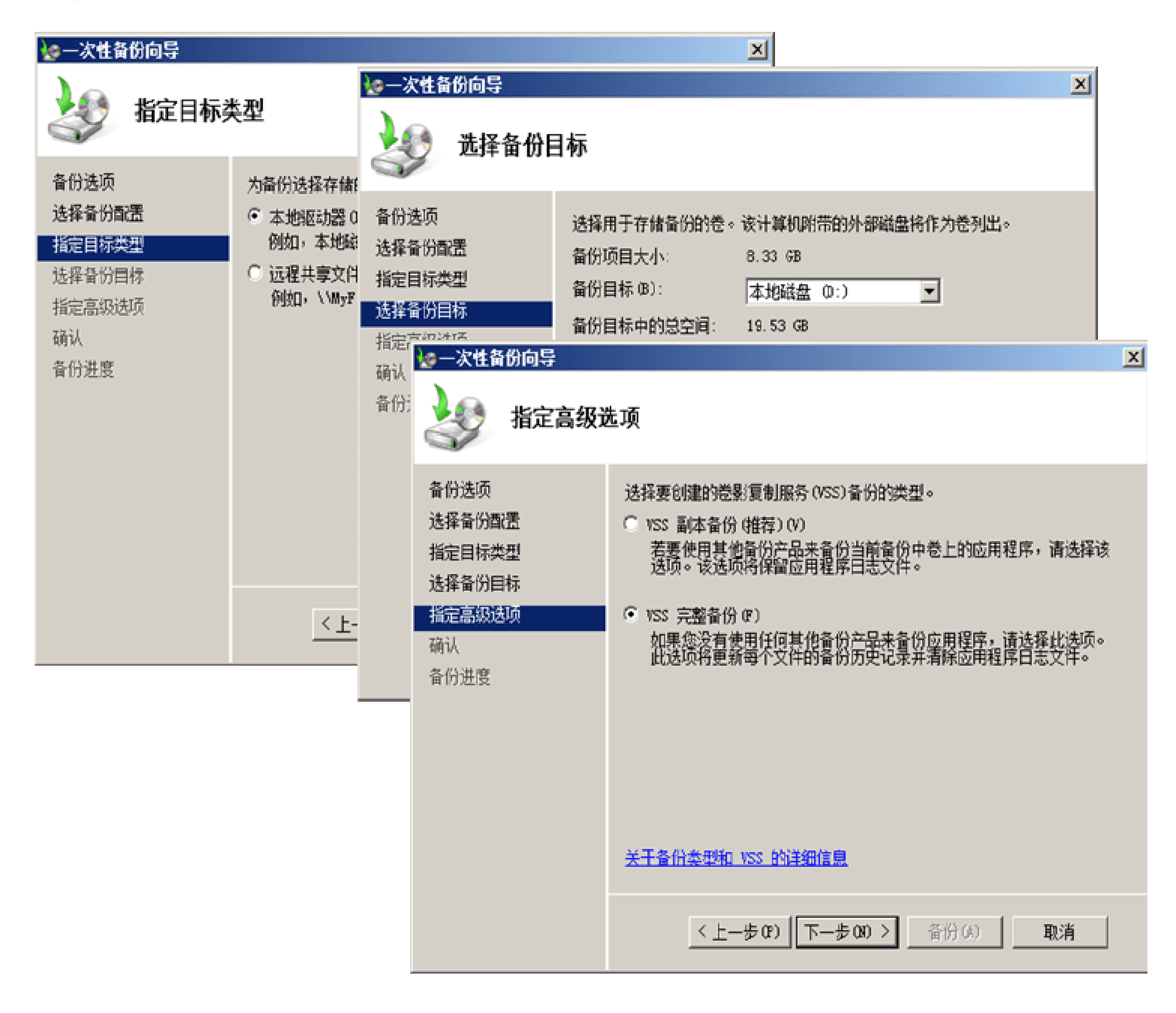


图 9.3　完成备份向导

2. 还原 Active Directory 数据库

Windows Server Backup 功能可以还原备份中的文件和文件夹，提供还原向导，管理员根据提示还原即可。还原 Active Directory 域控制器中的文件时，使用目录还原模式，确保域控制器中 Active Directory 数据库的安全。

01 重新启动计算机，在进入 Windows Server 2008 的初始窗口前，按 F8 键进入“高级启动选项”菜单界面。通过键盘上的方向键选择“目录服务还原模式”选项，如图 9.4 所示。



图 9.4　高级启动选项

02 加载操作系统文件，出现 Windows Server 2008 登录窗口，在“用户名”文本框中，输入“.\Administrator”登录到本机，在“密码”文本框中，输入目录还原模式密码，如图 9.5 所示。

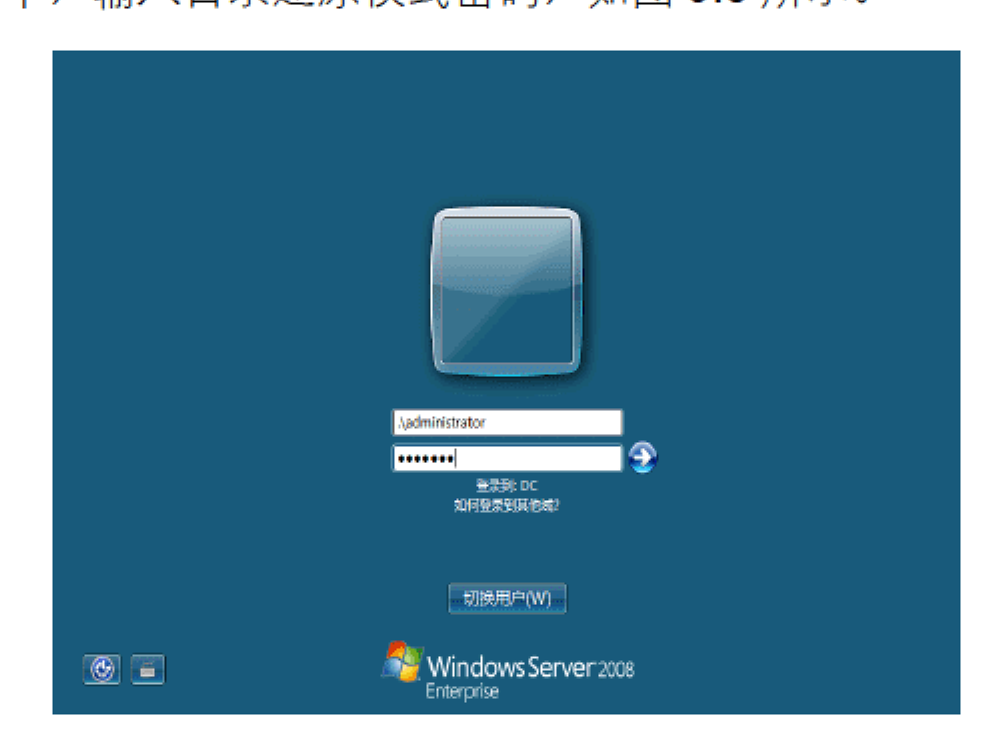


图 9.5　登录到本地计算机

03 启动完成，Windows Server 2008 系统处于安全模式，显示如图 9.6 所示窗口。

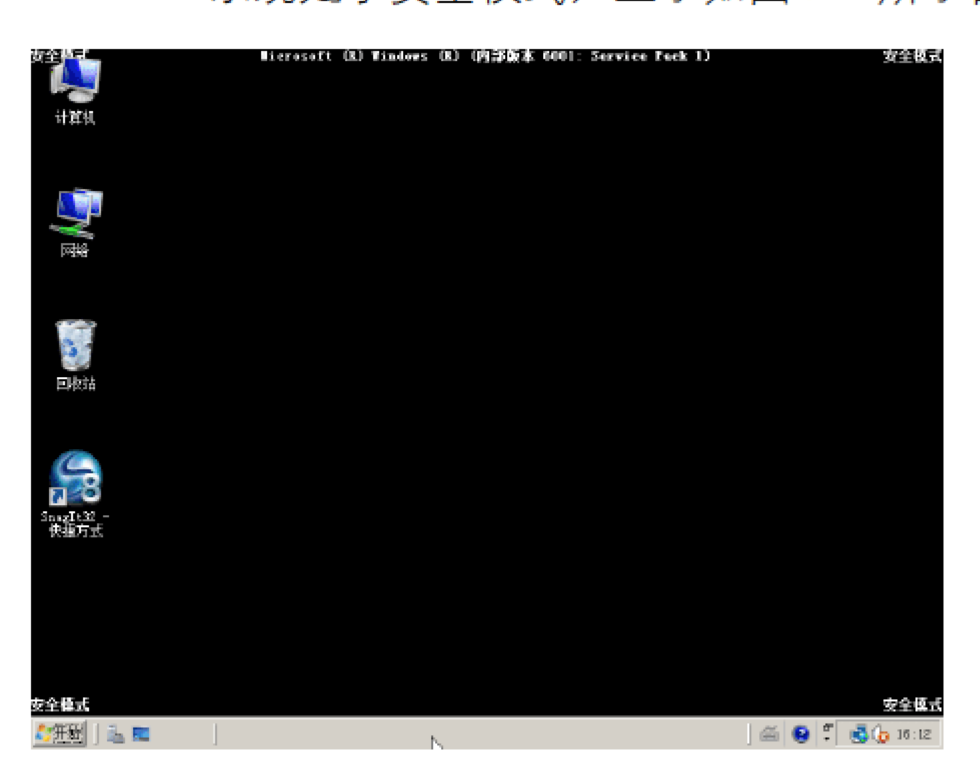


图 9.6　进入系统

04 依次选择“开始”→“管理工具”→“服务器管理器”→“存储”→“Windows Server Backup”选项，打开“Windows Server Backup”窗口。在右侧“操作”面板中，单击“还原”链接，显示如图 9.7 所示“入门”对话框。选择需要还原的目标服务器，本例选择“此服务器”选项。

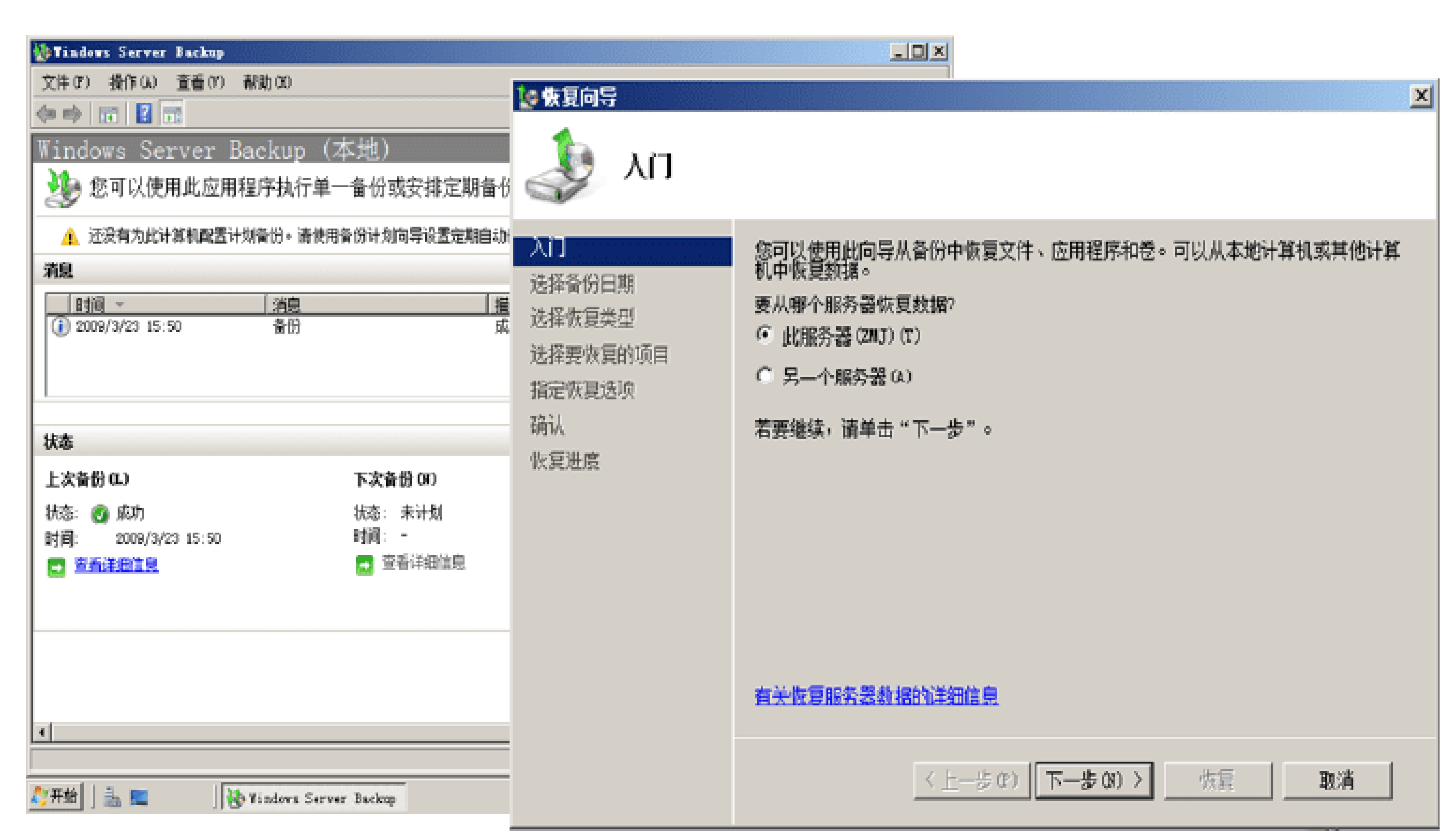


图 9.7　启动还原向导



05 依次单击“下一步”按钮，选定希望还原备份的日期和还原类型，如图 9.8 所示。在“选择备份日期”对话框中，选择备份内容以及备份时间。在“选择恢复类型”对话框中，提供“文件和文件夹”和“卷”还原选项，选择“文件和文件夹”单选按钮即可。

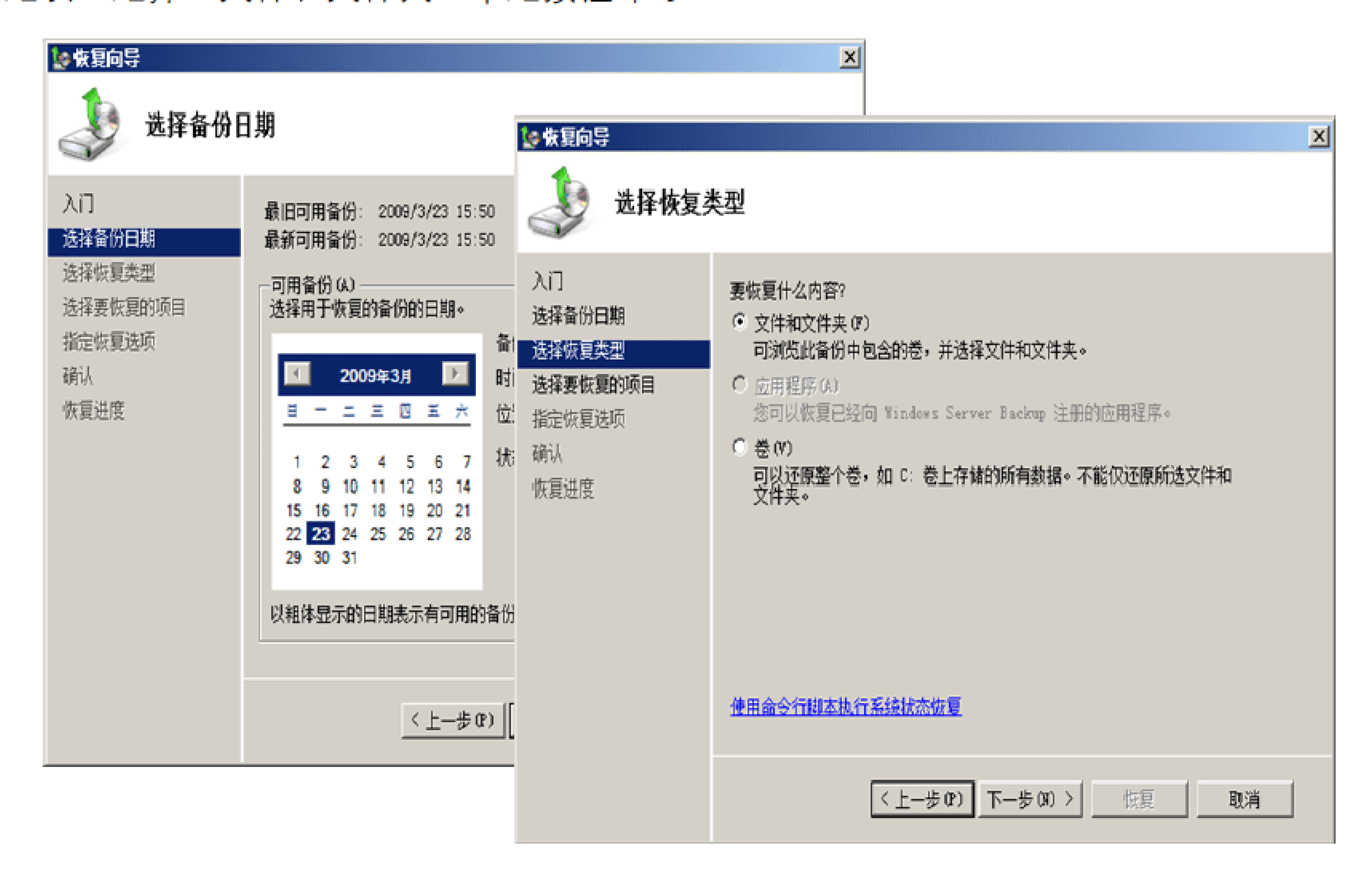


图 9.8　选择还原备份日期和恢复类型

06 单击“下一步”按钮，显示如图 9.9 所示“选择要恢复的项目”对话框。在“可用项目”列表中，选择需要还原的目标文件夹，在右侧的列表中显示选择的文件夹中包含的文件，管理员可以选择一个文件或者多个文件，选择的文件以高亮显示。

07 单击“下一步”按钮，显示如图 9.10 所示“指定恢复选项”对话框。将选择的文件还原的目标文件夹，可以还原到原始位置或者重定向到新的位置。如果在目标文件夹中，已经存在同名文件时，管理员可以根据需要选择创建文件副本还是覆盖文件或者不恢复文件和文件夹。



图 9.9　“选择要恢复的项目”对话框



图 9.10　“指定恢复选项”对话框

08 单击“下一步”按钮，显示“确认”对话框，显示恢复文件的恢复目标、恢复选项、安全设置等选项。单击“还原”按钮，执行文件还原，还原完成后显示如图 9.11 所示“恢复进度”对话框。完成后，单击“关闭”按钮，退出向导即可。



图 9.11　恢复备份文件

9.1.2　DHCP 服务器

在规模较大的局域网中，通常采用 DHCP 服务器为客户机统一分配 TCP/IP 配置信息。一旦出现人为的误操作或其他因素，将会导致 DHCP 服务器的配置信息出错或丢失，导致企业的员工不能正常工作。手工进行还原非常麻烦，而且工作量较大，同时 DHCP 服务器中可能包含多个作用域，并且每个作用域中又包含不同的 IP 地址段、网关地址、DNS 服务器等参数。因此，备份这些配置信息，就成为网络管理员的必要工作。

1. 备份 DHCP 数据库

在 DHCP 服务器中，已经内置了备份和还原功能，而且操作也非常简单。

01　在 DHCP 控制台窗口中，右击“DHCP 服务器名”选项，从快捷菜单中选择“备份”选项，显示如图 9.12 所示“浏览文件夹”对话框，指定备份文件的存放路径即可。



图 9.12　存放 DHCP 备份文件的位置



02 单击“确定”按钮，即可完成 DHCP 服务器配置信息的备份工作。

2. 还原 DHCP 数据库

01 如果 DHCP 配置信息损坏，需要进行还原时，可以右击“DHCP 服务器名”选项，从快捷菜单中选择“还原”选项，显示如图 9.13 所示“浏览文件夹”对话框，用户根据备份文件的路径来指定备份文件所在的路径。

02 单击“确定”按钮后，显示“DHCP”信息提示对话框，如图 9.14 所示。为了使改动生效，必须停止 DHCP 服务并重新启动该服务。

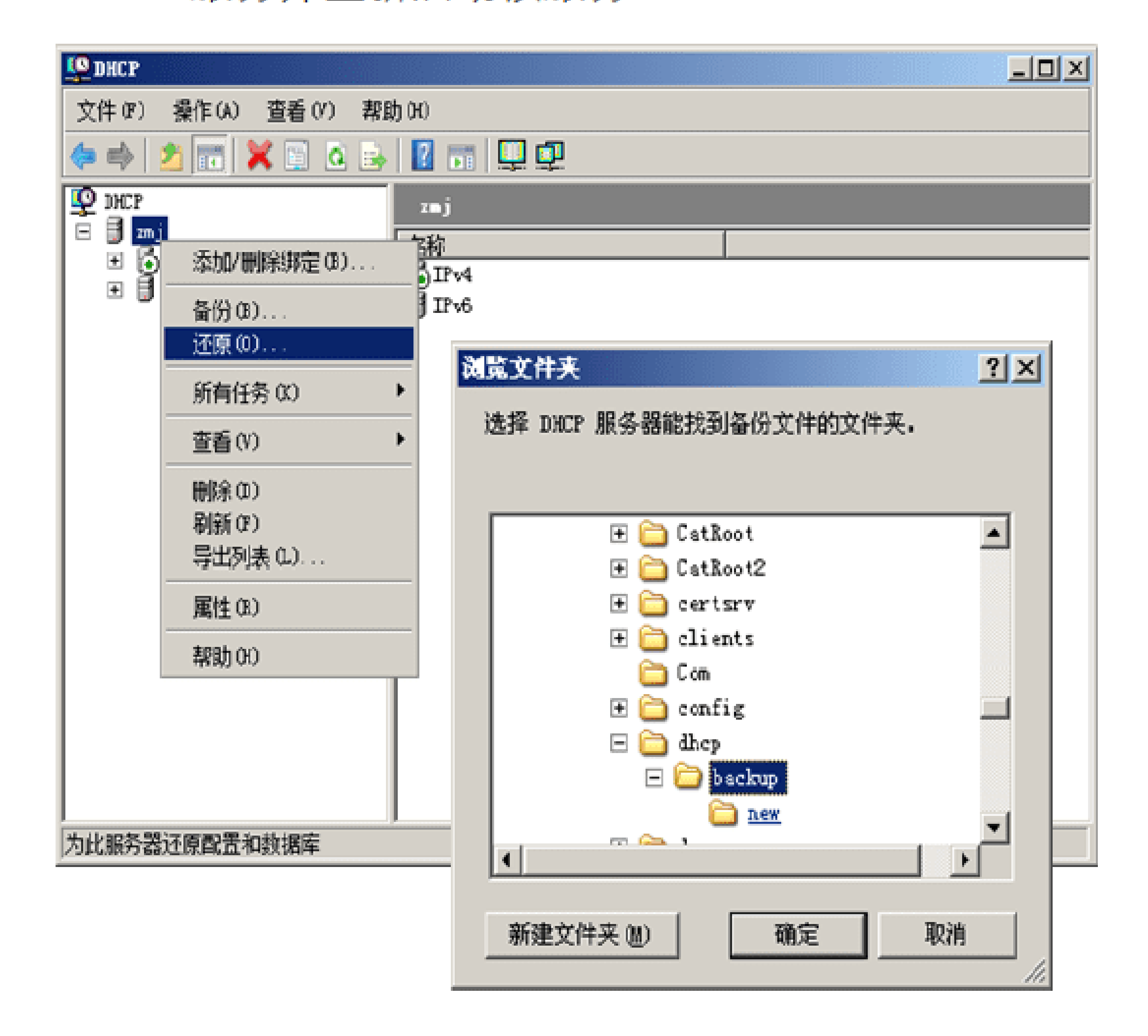




图 9.13　还原 DHCP 数据库　　　　图 9.14　DHCP 提示信息

9.1.3　DNS 服务器

DNS 服务器担负着域名解析的工作，其重要性不言而喻。如果网络中的 DNS 服务器出现问题或者信息数据丢失的话，则服务器就将无法完成域名的解析工作。因此，平时要经常对 DNS 服务器的数据信息进行备份。当发现 DNS 服务器出现问题时，可以方便的使用备份文件快速还原 DNS 服务器的工作。DNS 服务器数据的备份，分两步进行：首先，要备份注册表中的 DNS 服务器的相关信息；其次，要备份域名解析时所使用的 DNS 数据信息。

1. DNS 注册表信息备份

（1）备份 DNS 服务信息

01 打开注册表编辑器，在左侧的层次列表中依次展开“HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\DNS”项目，只要将此键值下的所有数据备份出来即可。

02 选中“DNS”项目，单击“文件”菜单中的“导出”选项，显示“导出注册表文件”对话框，指定备份文件的存放路径和文件名即可，如图 9.15 所示。

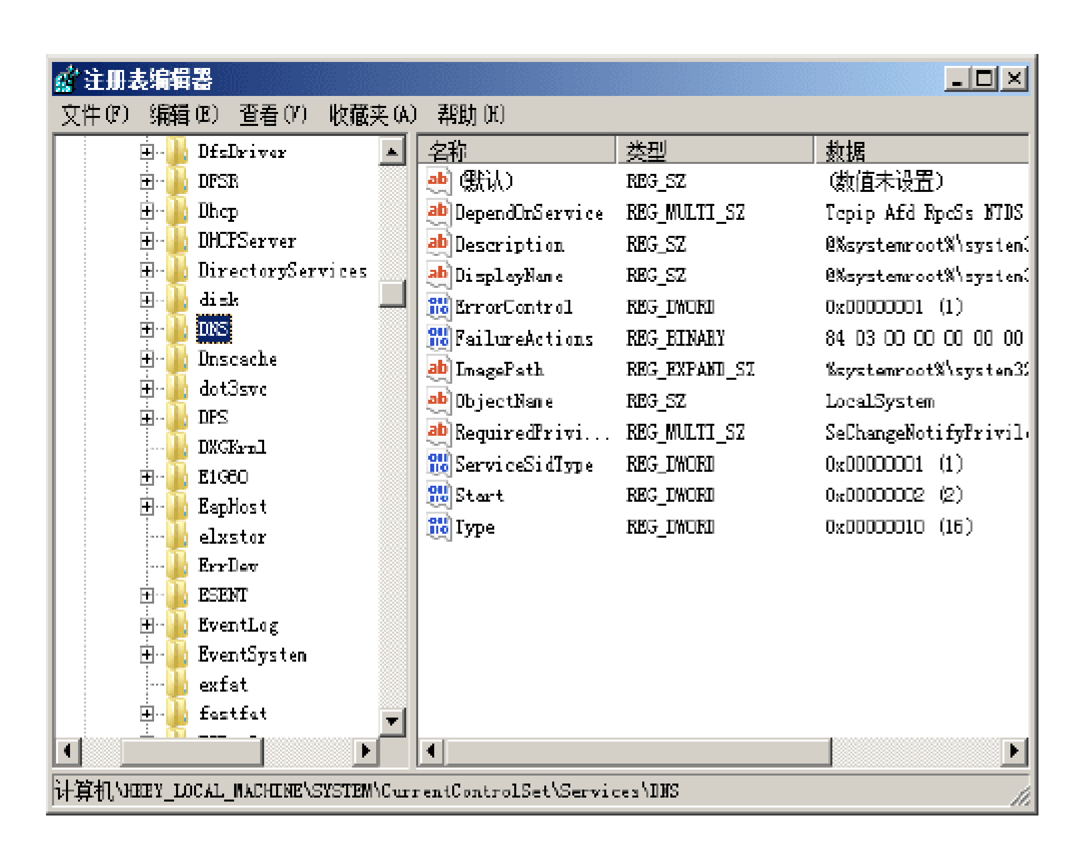


图 9.15 备份注册表的 DNS 服务信息



注意　在备份服务状态的时候，其实就已经备份了 DNS 信息，但是为了备份和还原 DNS 数据的简易性和方便性，建议对 DNS 数据进行单独备份。

（2）备份 DNS Server 服务信息

01 打开注册表编辑器，在左侧的层次列表中依次展开“HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\DNS Server”项目，将此键值下的所有数据备份出来即可。

02 选中“DNS Server”项目，单击“文件”菜单中的“导出”选项，显示“导出注册表文件”对话框，指定备份文件的存放路径和文件名称即可完成数据的保存，如图 9.16 所示。

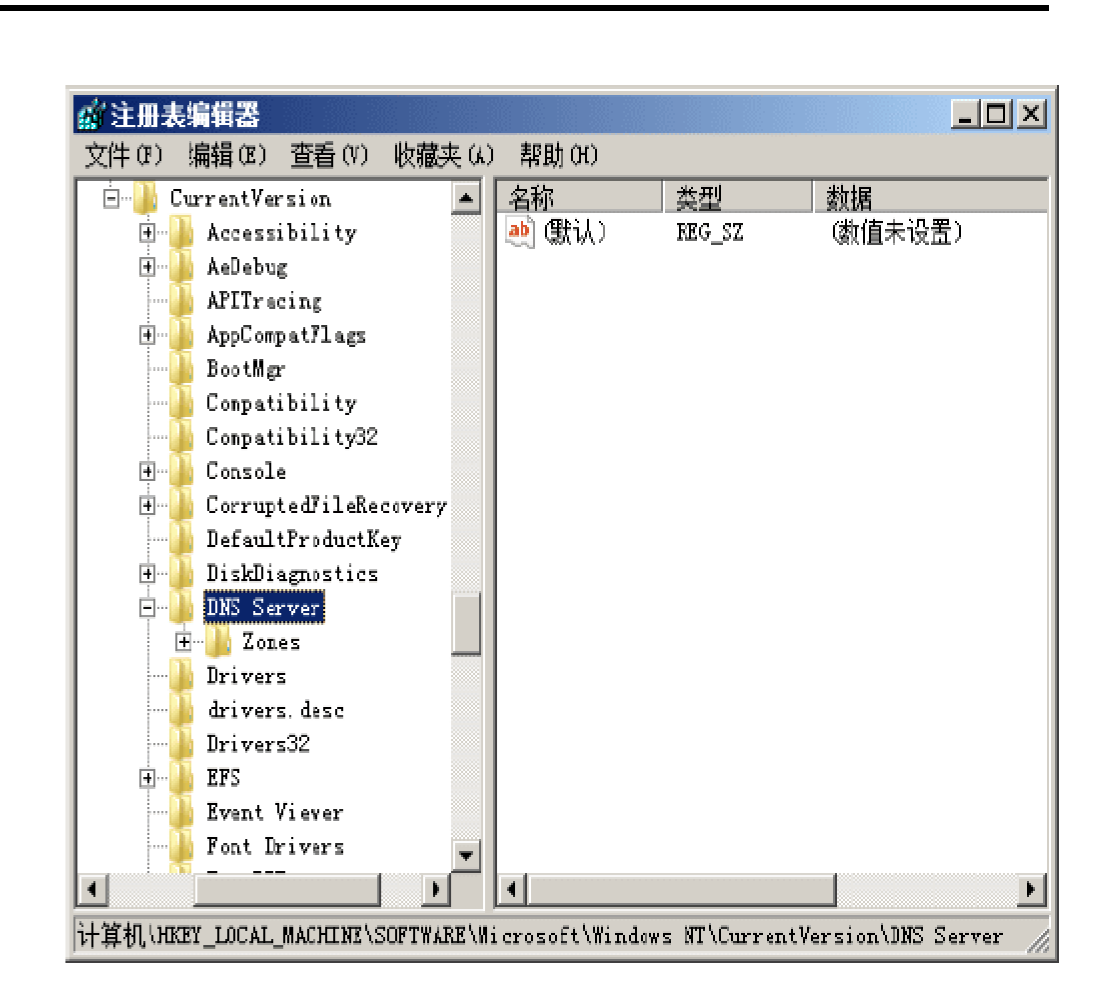


图 9.16 备份注册表的 DNS Server 服务信息

2. DNS 数据文件备份

“DNS 注册表信息备份”部分备份的是注册表中的信息，但其中并不包含域名解析时所使用的域名数据信息——这部分内容需要单独进行备份。

打开 DNS 服务器的资源管理器，进入到“c:\windows\system32\dns”目录，将后缀为“.dns”的所有文件备份出来，这些文件中存储的就是域名解析时所使用的域名数据信息，这样就完成了域名数据的备份操作，如图 9.17 所示。

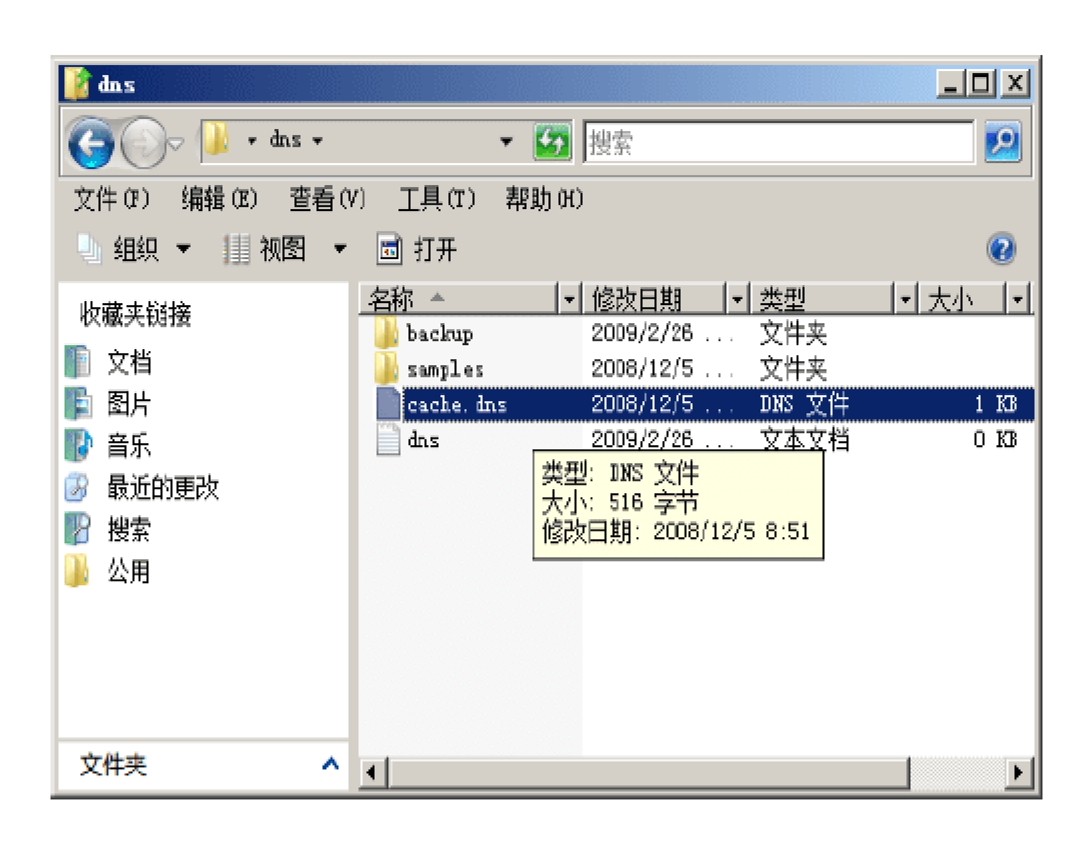


图 9.17 备份 DNS 数据文件



3. DNS 数据还原

当 DNS 服务器出现问题，可以使用备份的两部分数据进行还原。

01 运行备份的两个注册表文件，将其导入到注册表中。

02 将后缀为“.dns”的所有文件覆盖“c:\windows\system32\dns”目录下所有的同名文件，即可完成 DNS 服务器的数据还原。

注意　在完成还原 DNS 服务器的工作后，建议重新启动 DNS 服务器。

9.1.4　WINS 服务器

Windows Server 2008 添加 WINS 服务器功能之前，需要设置一个静态 IP。如果 WINS 服务器使用动态 IP，地址会发生改变，WINS 客户端就需要不断地重新配置。因为用户是根据 WINS 服务器的 IP 来配置客户端的。

1. 备份 WINS 数据库

01 选择“开始”→“管理工具”→“WINS”命令，打开“WINS”窗口。在左侧窗格中选择并右击“WINS 服务器”选项，在弹出的快捷菜单中选择“备份数据库”命令，打开如图 9.18 所示“浏览文件夹”对话框，选择 WINS 数据备份的位置。

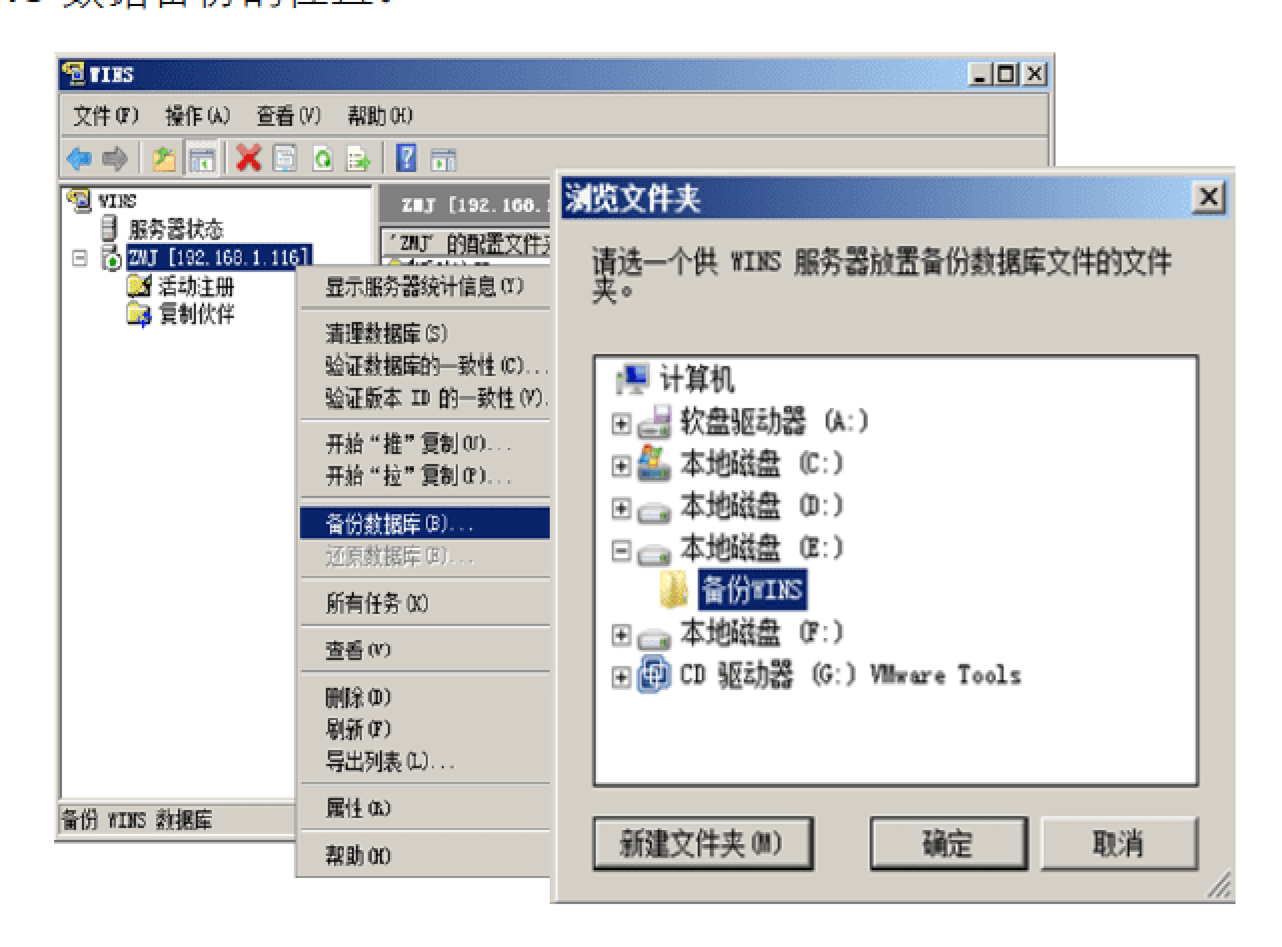


图 9.18　备份 WINS 服务数据库

02 单击“确定”按钮。备份过程完成之后，单击“确定”按钮即可完成 WINS 数据库的备份。

2. 还原 WINS 数据库

01 选择并右击左侧窗格中使用的 WINS 服务器。在弹出的快捷菜单中选择“还原数据库”命令。系统显示“浏览文件夹”对话框。

02 选择 WINS 数据库还原的位置。单击“确定”按钮。还原过程完成之后，重新启动 WINS 服务即可完成 WINS 的还原。

9.2 注册表的备份与还原

注册表是系统的重要数据库，如果出现错误，轻者造成系统启动错误或软件不能使用，重者造成系统整个瘫痪。由于应用程序和硬件配置经常修改注册表并增加内容，因此注册表比计算机中的其他静态的文件更容易出错或受到损坏。因此，定期维护、备份注册表是每位用户需要养成好习惯。

- 定期备份。根据用户使用电脑的情况，通常选择每周或每月进行一次，确保系统出错时能还原到最新的注册表状态。
- 增加硬件。当安装新硬件时，可能其驱动程序会与系统不兼容，造成系统瘫痪，为预防此故障，应事先备份注册表。
- 安装软件。当需要安装未使用过的软件时，防止其与系统中的其他软件相冲突，造成系统瘫痪，需要事先备份好注册表。

9.2.1 备份注册表

以管理员身份登录系统，依次选择“开始”→“运行”命令，在“运行”对话框中输入“regedit”命令，单击“确定”按钮，打开“注册表编辑器”窗口。依次选择“文件”→“导出”命令，显示“导出注册表文件”对话框。选择注册表备份文件的保存路径、名称以及保存全部还是只保存注册表的某个分支。单击“保存”按钮即可完成注册表的备份，如图 9.19 所示。

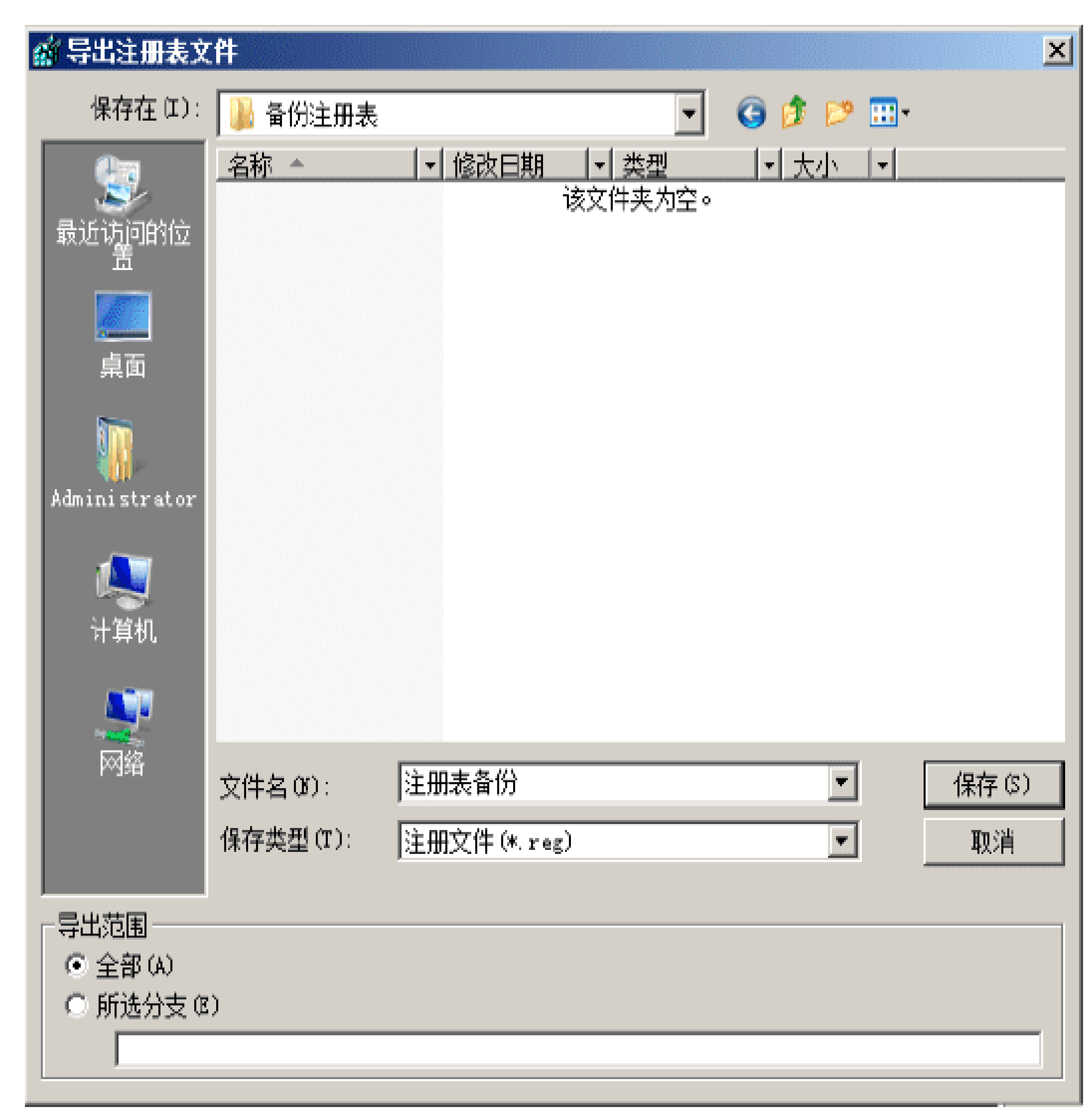


图 9.19 “导出注册表文件”对话框

9.2.2 还原注册表

在“注册表编辑器”窗口中，依次选择“文件”→“导入”命令，显示“导入注册表文件”对话框，浏览曾经导出的注册表备份文件，单击“打开”按钮即完成注册表的还原，如图 9.20 所示。还原完成后需要重新启动计算机，按照提示操作即可。



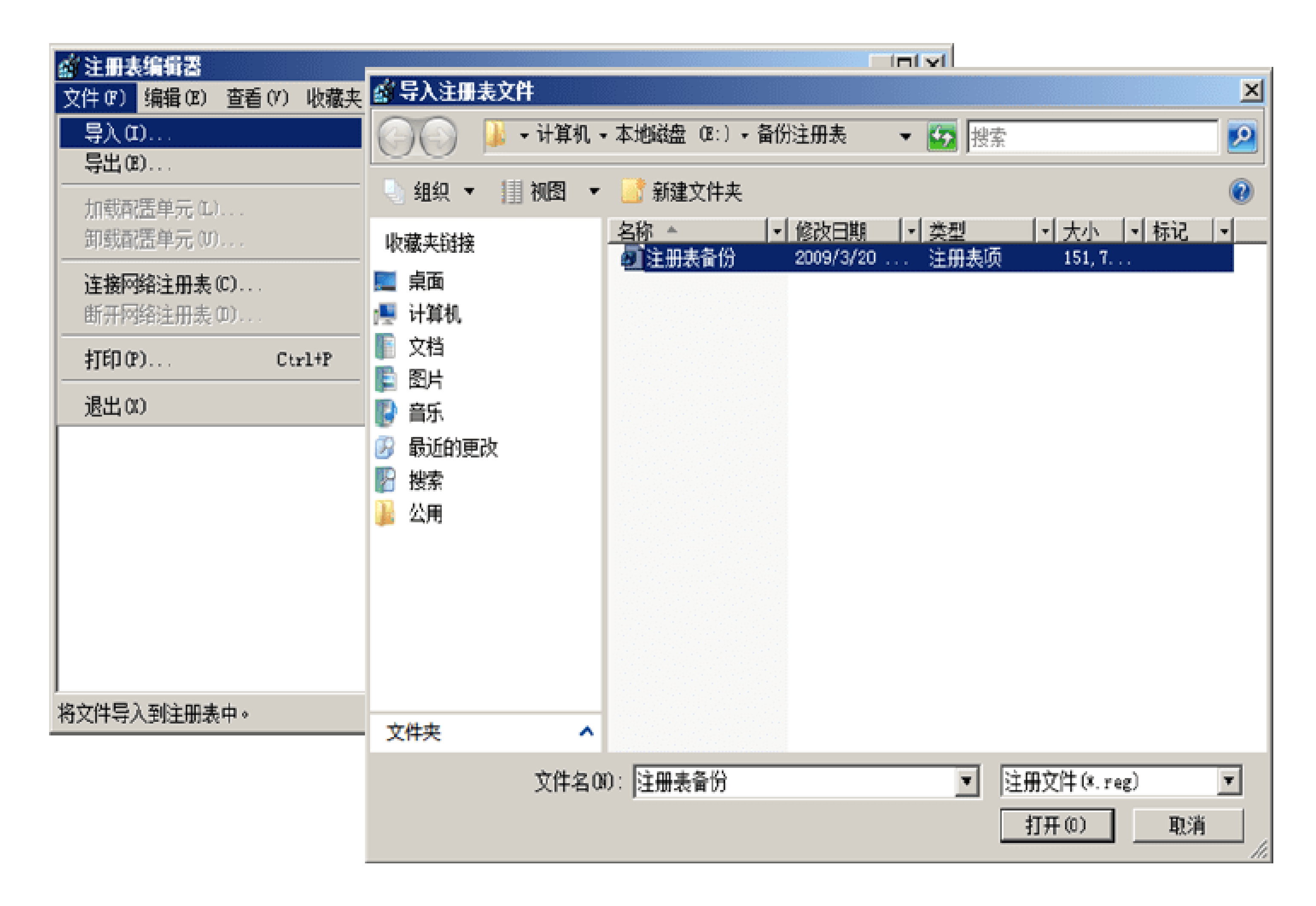


图 9.20　打开“导入注册表文件”对话框

9.3　网络配置的备份与还原

作为一名网络管理员，首先要能够维护网络安全正常的运行，在网络发生故障时能迅速进行还原。在网络故障还原过程中，尤为重要的是服务器网络设置的还原。Netsh 是 Windows 2000/XP/2003/Vista/2008 操作系统自身提供的命令行脚本实用工具，允许用户在本地或远程，显示和修改当前正在运行的计算机的网络配置，另外也可以将配置脚本保存在文本文件中。

9.3.1　备份服务器的网络设置

常规服务器的网络设置包括IP地址设置、接口、端口代理、远程访问、路由、DNS 代理、NAT、DHCP 中继代理配置等。这些网络参数的设置，根据服务器在网络中所起的特殊作用而有所不同。只有对网络服务器的设置进行了相应的备份，才能在网络设置遇到毁灭性破坏时，迅速并且及时地还原网络。

在命令行模式下输入如下命令：

```
netsh dump >d:\NFC-lxh-2008.txt
```

回车确认，命令行成功执行，将网络设置备份到“c:\bak1txt”文件中，该文件为一个文本文件，如图 9.21 所示。

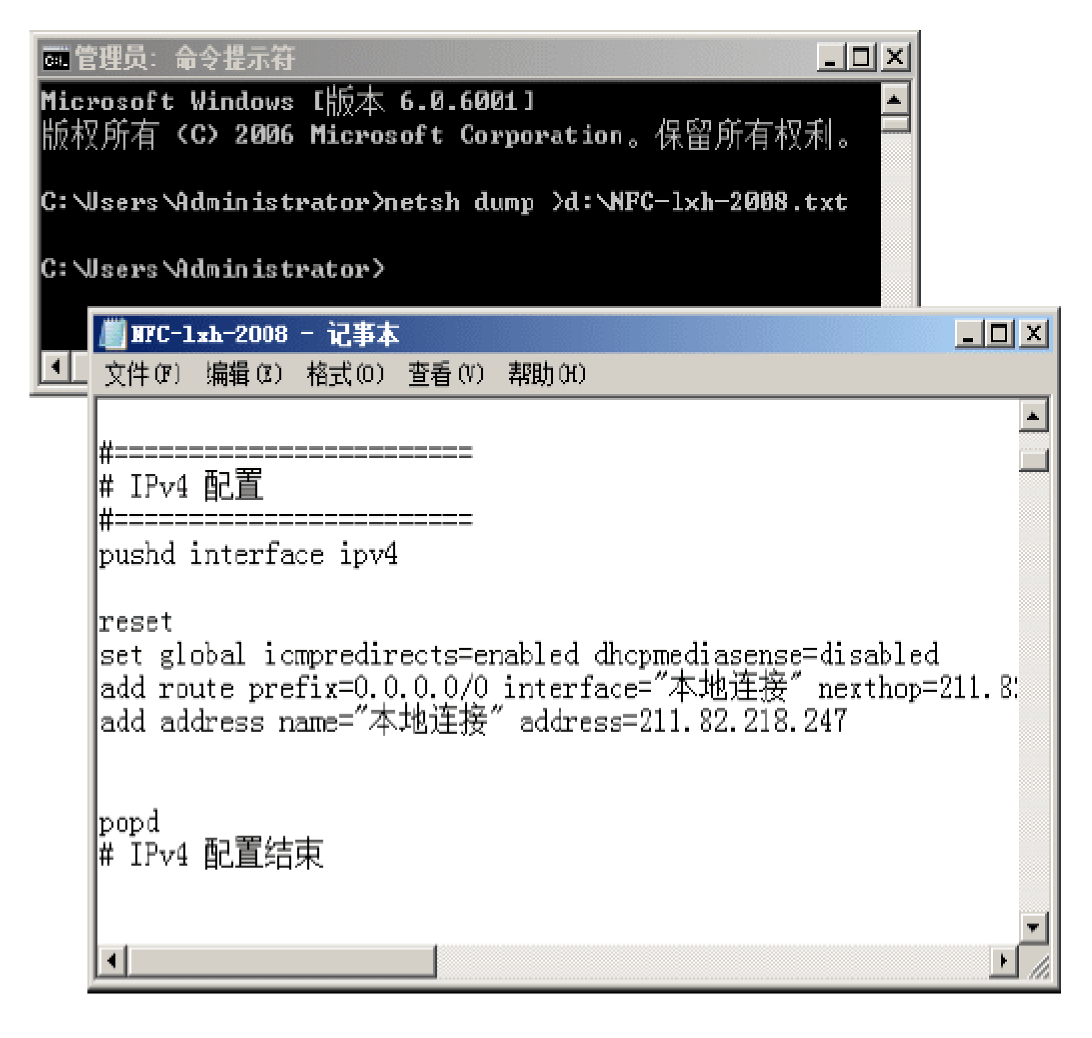


图 9.21　备份服务器的网络设置

9.3.2　还原服务器的网络设置

在进行网络设置调整时，如果发生了操作失误，或者服务器的网络发生故障，可以利用备份快速还原网络设置。

在命令行模式下输入如下命令：

```
Netsh exec d:\NFC-lxh-2008.txt
```

回车确认，命令成功执行，即可将已经备份好的网络设置还原到系统中。该命令非常适合网络管理人员用来对服务器网络设置进行备份和还原管理。

9.4　磁盘配额的备份与还原

使用 Windows 系统提供的磁盘配额功能，对每个用户所使用的磁盘容量进行限制。但是如果服务器由于某些原因，或者因为重新安装服务器操作系统和其他原因造成配置信息丢失，那么手工还原起来就需要大量时间。因此网络管理员在备份系统服务的同时，还应备份好磁盘配额项目的信息。

9.4.1　备份磁盘配额

01 右击启用磁盘配额的分区（以 D 盘为例），选择快捷菜单中的“属性”选项，切换到“配额”选项卡，单击“配额项”按钮，显示如图 9.22 所示“（D:）的配额项”对话框。

02 右击希望备份的配额项目，并选择“导出”选项，显示“导出配额设置”对话框。指定保存备份文件的目录后单击“确定”按钮，即可开始备份。也可以同时导出多个配额项目。



图 9.22　“（D:）的配额项”对话框

9.4.2　还原磁盘配额

在配额项目管理对话框中，单击“配额”→“导入”选项，即可选择已保存的备份文件。还原磁盘配额设置时，系统会显示如图 9.23 所示“磁盘配额”对话框。单击“是”按钮，即可完成磁盘配额项目的还原。

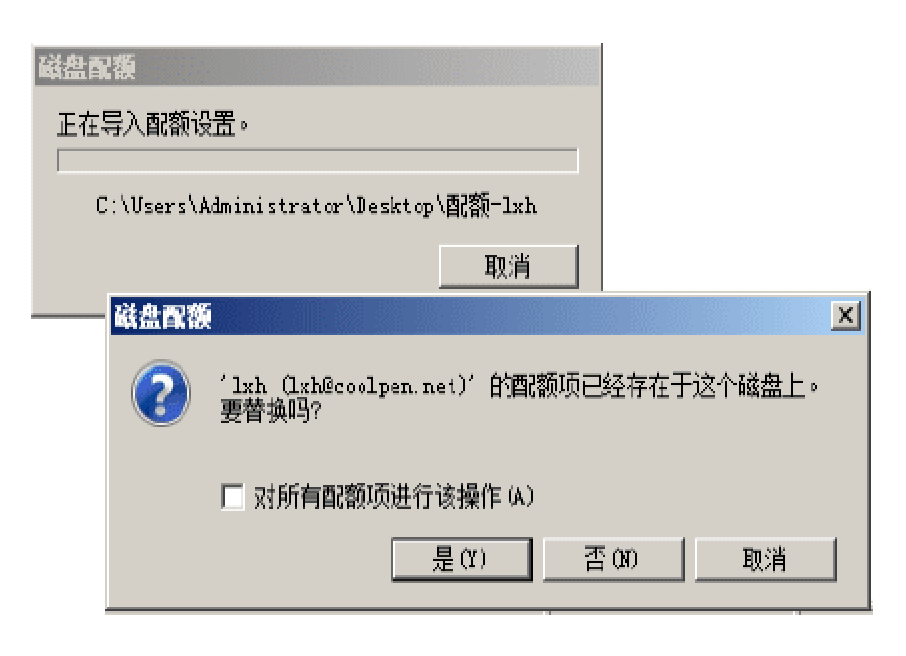


图 9.23　“磁盘配额”对话框



小　　结

文件安全是系统安全中最重要的课题之一，为了防止系统问题而导致数据丢失，可以对重要数据进行安全备份与还原。系统数据备份的内容非常广泛，管理员可以对系统账号、注册表、WINS 服务器信息进行备份，甚至还可以备份收藏夹、输入法和系统字体，备份和还原操作简单，适合管理员统一备份和用户自主备份。

习　　题

1. 系统备份有哪些类型？
2. 如何对系统账号进行备份和还原？
3. 如何使用 Windows Server Backup 备份 Active Directory 数据库？
4. 如何对注册表进行备份和还原？

实验：备份和还原服务器网络配置信息

实验目的

掌握运用 netsh 命令快速备份和恢复服务器的网络配置信息。

实验内容

备份网络配置信息后，更改其 IP 地址和子网掩码，然后使用备份文件恢复配置信息。

实验步骤

1. 查看服务器当前网络配置信息。
2. 使用 netsh dump 命令导出网络配置。
3. 更改服务器 IP 地址和子网掩码。
4. 使用 netsh exec 命令恢复网络配置。
5. 验证服务器网络配置信息，是否成功恢复。

Windows Server 2008

第10章

电子证书和认证服务

随着网络应用技术的发展，安全隐患也越来越多，尤其是在一些未经允许授权用户访问的网络，一旦数据被人截获、篡改或假冒等，对企业和用户都带来难以想象的恶劣后果。因此，安全问题也越来越被人们所重视，特别是电子交易网站。而电子证书是一种应用非常广泛的提高通信安全性的方式，可以实现用户身份认证、数据加密等功能，从而保护用户的网络及传输信息的安全。

本章导读

- 安装证书服务
- 企业证书服务器的应用
- 独立证书服务器的应用
- 证书服务器的备份、还原与管理



10.1　电子证书和认证服务概述

要利用电子证书实现网络安全通信，必须要搭建认证服务器。安全 Web 连接的站点（使用 HTTPS）、邮件的签名和加密、网上银行在线交易等都需要证书来保护用户或计算机的安全。Windows Server 2008 自带了证书服务功能，可以实现不同类型数字证书的颁发，用户使用所颁发的证书即可实现安全连接、数据加密等功能。

10.1.1　数字证书简介

电子证书类似于生活中的“证书”，都是由信任的证书颁发机构或第三方机构颁发的，并且不同的证书只能应用于其特定的领域。不过，电子证书则是一段由证书颁发机构（Certification Authority，简称 CA）数字签名的、包含用户身份信息和用户公钥信息以及身份验证机构数字签名的数据，用来代表用户的身份。其中，身份验证机构的数字签名可以确保证书信息的真实性，而用户公钥信息可以保证数字信息传输的完整性，用户的数字签名可以保证数字信息的不可否认性。

证书的主要功能是向网络上的其他用户证明个人身份、用于网络上身份验证及保证公开网络上信息安全。每个证书都拥有可以公开的“公钥”及与之相关联的私钥，同时只有证书持有人才拥有“私钥”。证书将公钥安全地绑定到持有相应私钥的实体中，并通过网络进行传输。证书由证书颁发机构进行管理，此过程称为“签名”。而且，证书可以颁发给用户、计算机或某一应用程序。

Windows Server 2008 使用公共密钥基础结构（PKI，Public Key Infrastructure）来处理企业内部或外部网络中用户的身份验证、数据加密、数字签名等。公共密钥属于“非对称加密”技术，使用“公钥”和“私钥”两个密钥。其中，“公钥”可以对所有用户公开；而“私钥”则必须由使用者自己秘密保存，不能泄漏。这两个密钥彼此相关联，通常都是通过证书来发布的。

用户在发送信息时，可以使用自己的“私钥”对发送的电子邮件、文档等进行“签名”，如果数据在传送的过程中被更改，则收到的电子邮件、文档中的“签名”信息将不复存在，而接收者也将看不到发送者的“签名”信息，这样接收者就可以判断所接收到的信息是否被“篡改”。当然，发送者也可以使用接收者的“公钥”对发送的数据进行“加密”，只有接收者使用自己的“私钥”才能解密，即使其他人通过各种途径收到该数据，由于没有对应的私钥所以不能查看数据内容，从而保证了数据的安全。

10.1.2　认证服务简介

Windows Server 2008 支持两种证书服务器，分别是应用于企业内部的企业证书服务器和

企业或 Internet 的独立证书服务器。其中，企业证书服务器应用于域环境，需要 Windows Server 2008 活动目录（Active Directory）的支持，用户可以直接向证书服务器申请并安装证书。独立根证书服务器应用于非域环境，可以安装在任何一台独立服务器上，但用户向证书服务器申请证书时，必须由管理员检查后颁发才能使用。

需要注意的是，在部署了证书服务以后，服务器的计算机名和域名都不能更改，但可以更改 IP 地址。

10.2 证书服务的安装

Windows Server 2008 支持两种证书服务，分别用于企业内部的企业证书服务器（企业 CA）和企业或 Internet 网络中的独立的证书服务器（独立 CA）。企业 CA 需要 Windows Server 2008 活动目录的支持，而独立 CA 则可以安装在任何独立的 Windows Server 2008 计算机中。

10.2.1 企业 CA 的安装

证书服务作为 Windows Server 2008 内置组件，默认情况下并没有安装。由于企业证书服务器需要活动目录的支持，因此，在安装企业证书服务器时必须先安装域服务。

01 运行“添加角色向导”，当显示“选择服务器角色”对话框时，在“角色”列表框中选中“Active Directory 证书服务”复选框，依次单击“下一步”按钮，查看 Active Directory 证书简介并选择希望安装的角色服务，如图 10.1 所示。在“选择角色服务”对话框中，可以选择为 Active Directory 证书服务安装的角色服务，默认选中“证书颁发机构”复选框。如果要启用证书 Web 注册功能，可同时选中“证书颁发机构 Web 注册”复选框，由于证书 Web 注册需要启用 Web 功能，因此需要同时添加 Web 服务器功能。



图 10.1 选择需要安装的角色服务



注意　只有 Windows Server 2008 企业版和数据中心版支持 Web 注册功能，标准版和 Web 版则不支持。

02 依次单击“下一步”按钮，设置安装类型、CA 类型和私钥，如图 10.2 所示。在“指定安装类型”对话框中，选择“企业”单选按钮，用来安装企业证书。在“指定 CA 类型”对话框中，选择“根 CA”单选按钮。在“设置私钥”对话框中，选择“新建私钥”单选按钮。



图 10.2　设置安装类型、CA 类型和私钥

03 依次单击“下一步”按钮，设置 CA 加密、CA 名称和有效期，如图 10.3 所示。在“为 CA 配置加密”对话框的“选择加密服务提供程序”下拉列表中，选择加密程序，在“密钥字符长度”下拉列表中可选择密钥长度，在“选择此 CA 颁发的签名证书的哈希算法”列表框中，选择要使用的哈希算法。在“配置 CA 名称”对话框中，设置此证书的公用名称。在“设置有效期”对话框中，设置该证书的有效期，默认为 5 年。

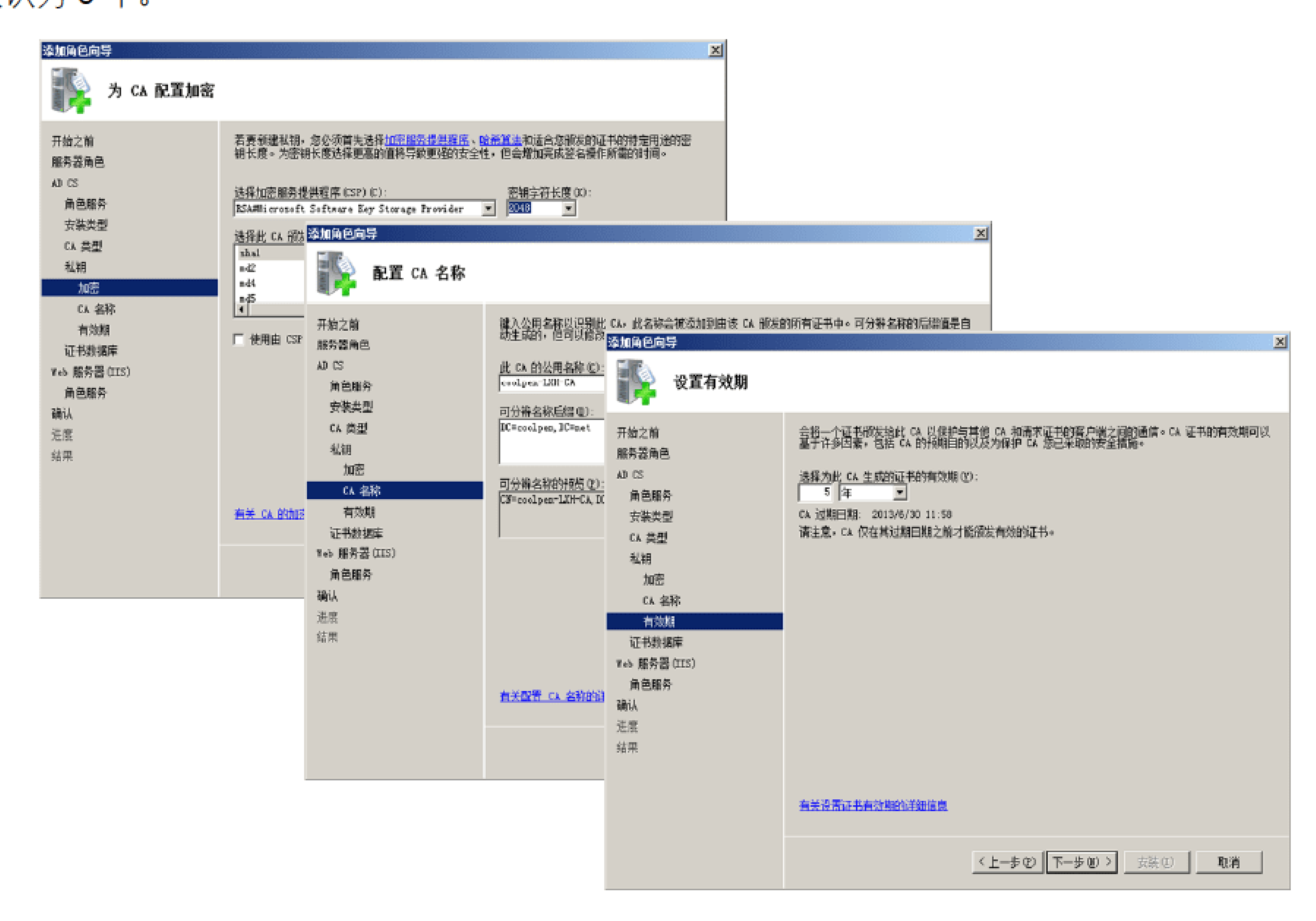


图 10.3　设置 CA 加密、CA 名称和有效期

04 依次单击“下一步”按钮，配置证书数据库、安装 Web 服务器直至安装完成，如图 10.4 所示。在“配置证书数据库”对话框，设置证书数据库和数据库日志的位置。在“Web 服务器（IIS）”对话框中，查看 IIS 的简介信息。在“选择角色服务”对话框中，用来选择欲安装的 IIS 组件。保持默认设置即可。



图 10.4　配置证书数据库、安装 Web 和 CA

05 单击“关闭”按钮，证书服务安装完成。打开“服务器管理器”窗口，依次展开“角色”→“Active Directory 证书服务”，即可查看所安装的证书服务，如图 10.5 所示。

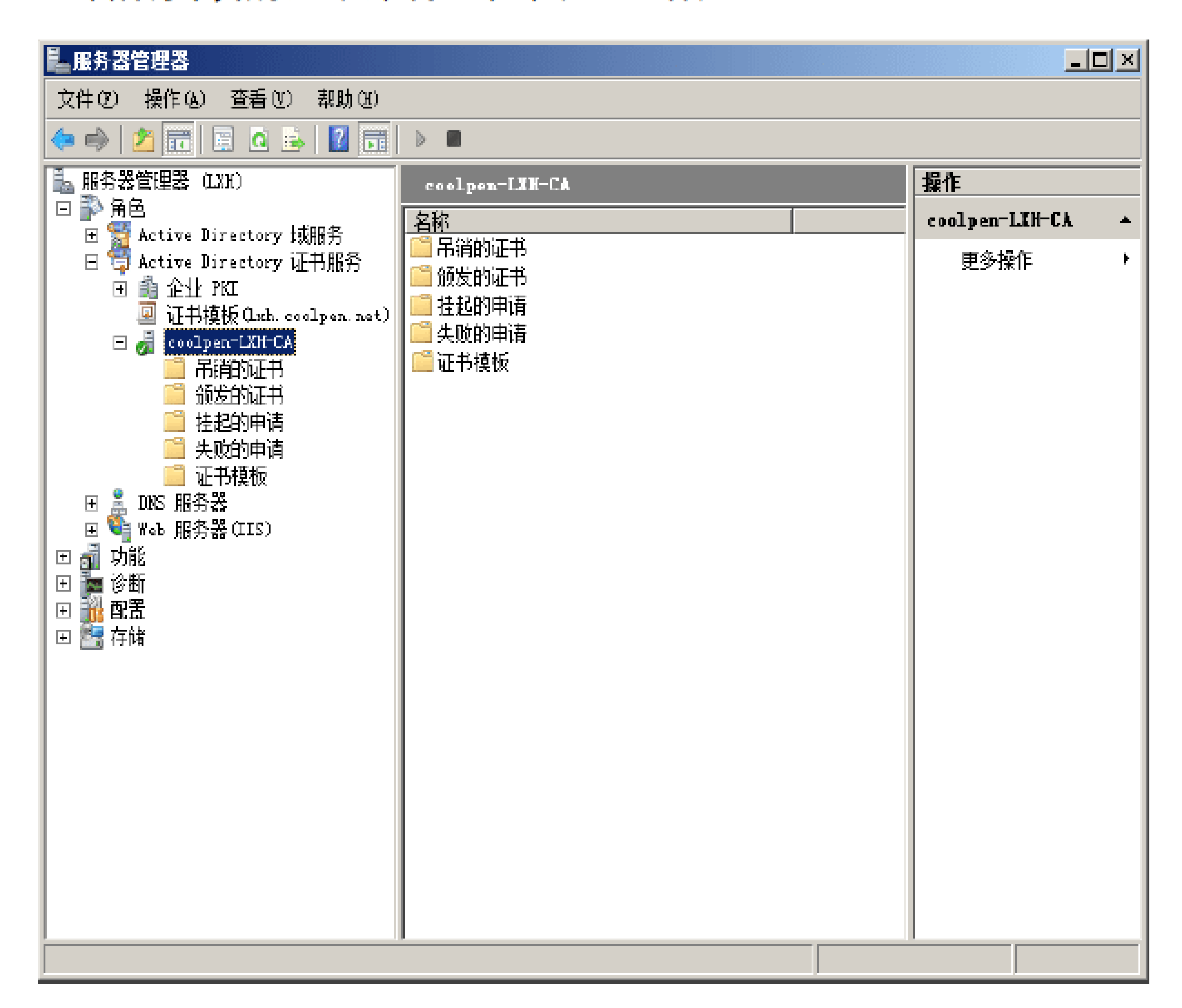


图 10.5　证书服务

10.2.2　独立根 CA 的安装

如果网络内尚未安装域服务，也可以将证书服务安装在独立服务器上，从而实现证书的颁发与管理。不过，由于独立根 CA 不需要 Active Directory，因此，只能使用 Web 方式注册证



书，无法利用“证书申请向导”，而且所申请的证书必须经由管理员颁发。

01 以管理员用户身份登录到服务器，运行“添加角色向导”，在“选择服务器角色”对话框中选中“Active Directory 证书服务”复选框。

02 在“选择角色服务”对话框中，同时选中“证书颁发机构”和“证书颁发机构 Web 注册”复选框，以启用 Web 注册功能，如图 10.6 所示。



图 10.6　“选择角色服务”对话框

03 在“指定安装类型”对话框中，选择“独立”单选按钮，如图 10.7 所示。由于此服务器不是域控制器，且未加入域，因此，“企业”单选按钮为灰色不可选状态。



图 10.7　“指定安装类型”对话框

04 其他操作，与安装企业 CA 时完全相同，这里不再赘述。

10.3　企业证书服务器的应用

企业证书服务器安装完成以后，无论是域成员用户，还是非域成员，都可以向证书服务器申请证书。申请证书可以使用 Web 方式或“证书申请向导”两种方式，前者无论是域成员还是非域成员都可使用，而后者只有加入域以后才能使用。

10.3.1　使用 Web 方式申请与安装证书

如果在安装证书服务器的同时，也安装了“证书颁发机构 Web 注册”，那么，就可以通过 Web 方式来申请证书，而且不需要加入域，但需要配置信任证书服务器才能安装证书。而对于域用户，则无需配置证书服务信任即可安装证书。申请证书的客户端可以使用 Windows 2000/XP/Vista 操作系统，这里以 Windows Vista 系统为例。

1. 配置 IE 浏览器

01 使用管理员用户登录 Windows Vista，首先需要使 IE 浏览器能够运行 ActiveX 控件。打开 IE 浏览器，单击“工具”菜单中的“Internet 选项”，选择“安全”选项卡，显示如图 10.8 所示。

02 单击“自定义级别”按钮，显示“安全设置－Internet 区域”对话框，将“对未标记为可安全执行脚本的 ActiveX 控件初始化并执行脚本（不安全）”和“允许运行以前未使用的 ActiveX 控件而不提示”均选择为“启用（不安全）”单选按钮，如图 10.9 所示。



图 10.8 “Internet 选项”对话框

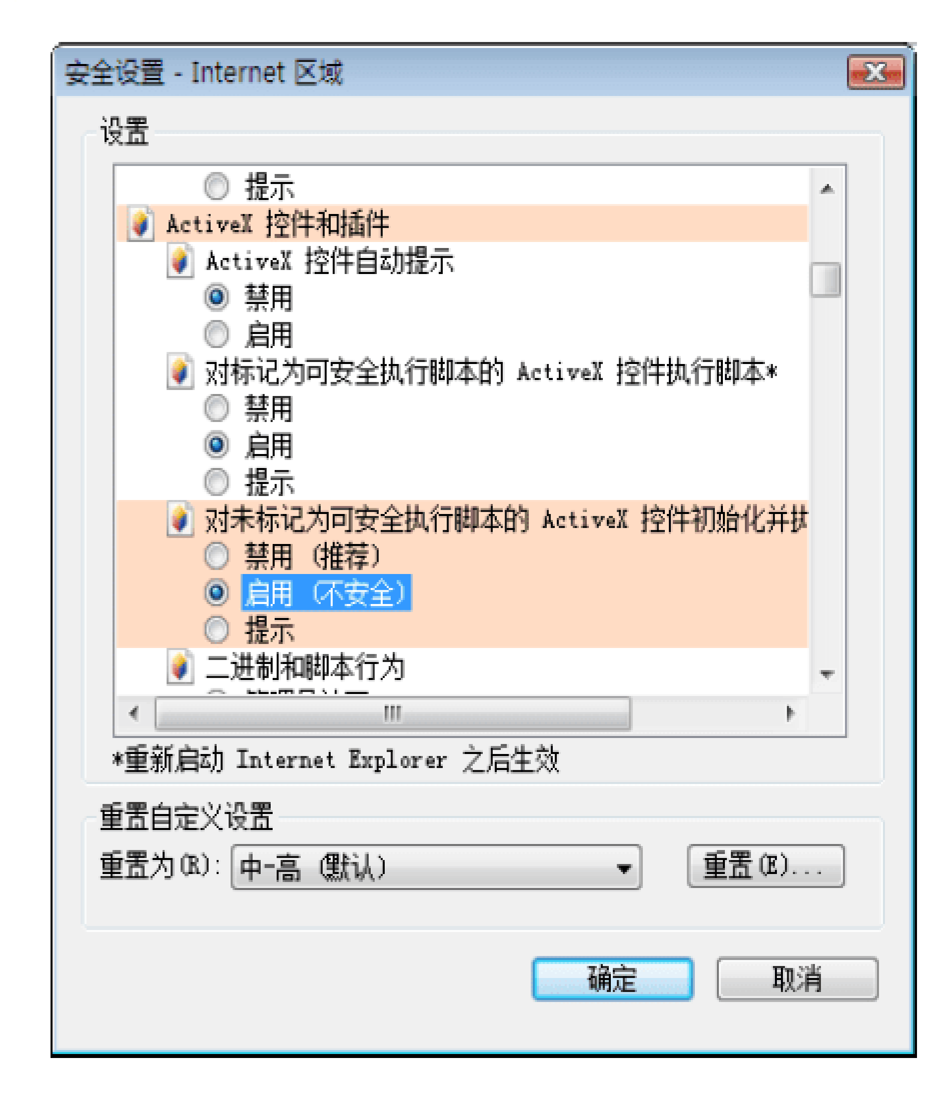


图 10.9 “安全设置–Internet 区域”对话框

注意 如果未在 IE 浏览器的安全设置中启用这两项，则在申请证书时就会显示如图 10.10 所示提示框。

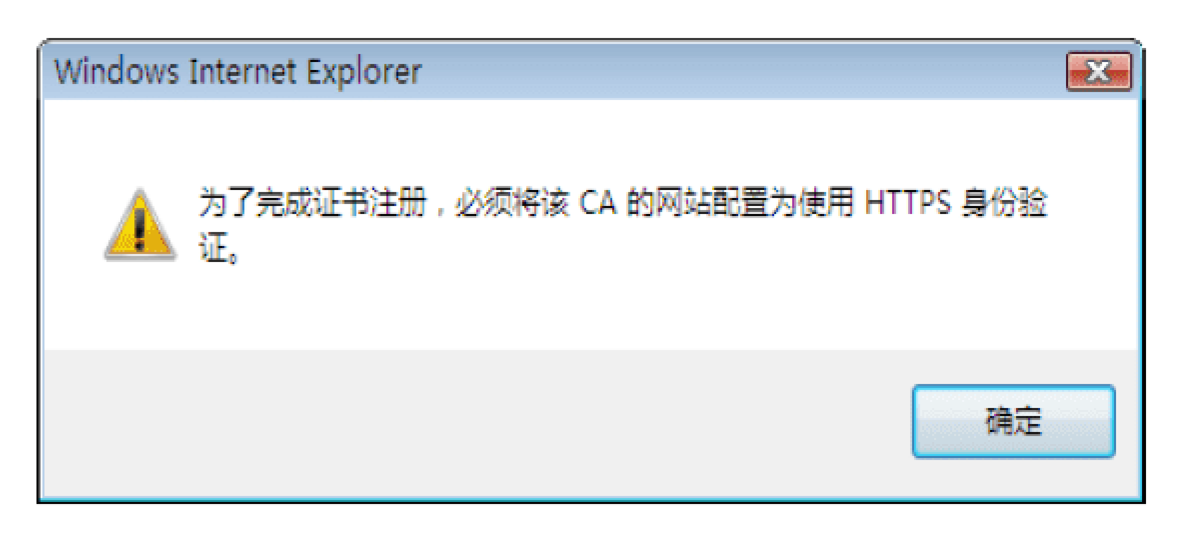


图 10.10 提示框

03 单击“确定”按钮保存即可。

2. 信任证书颁发机构

如果客户端计算机没有加入域，必须配置为信任证书颁发机构，才能安装从证书服务器申请的证书，否则，将无法安装。



01 打开 Web 浏览器，在地址栏中输入证书服务器的证书申请地址，格式为 http://证书服务器的 IP 地址/certsrv，例如：http://192.168.1.10/certsrv，回车，显示如图 10.11 所示“连接到”登录框。

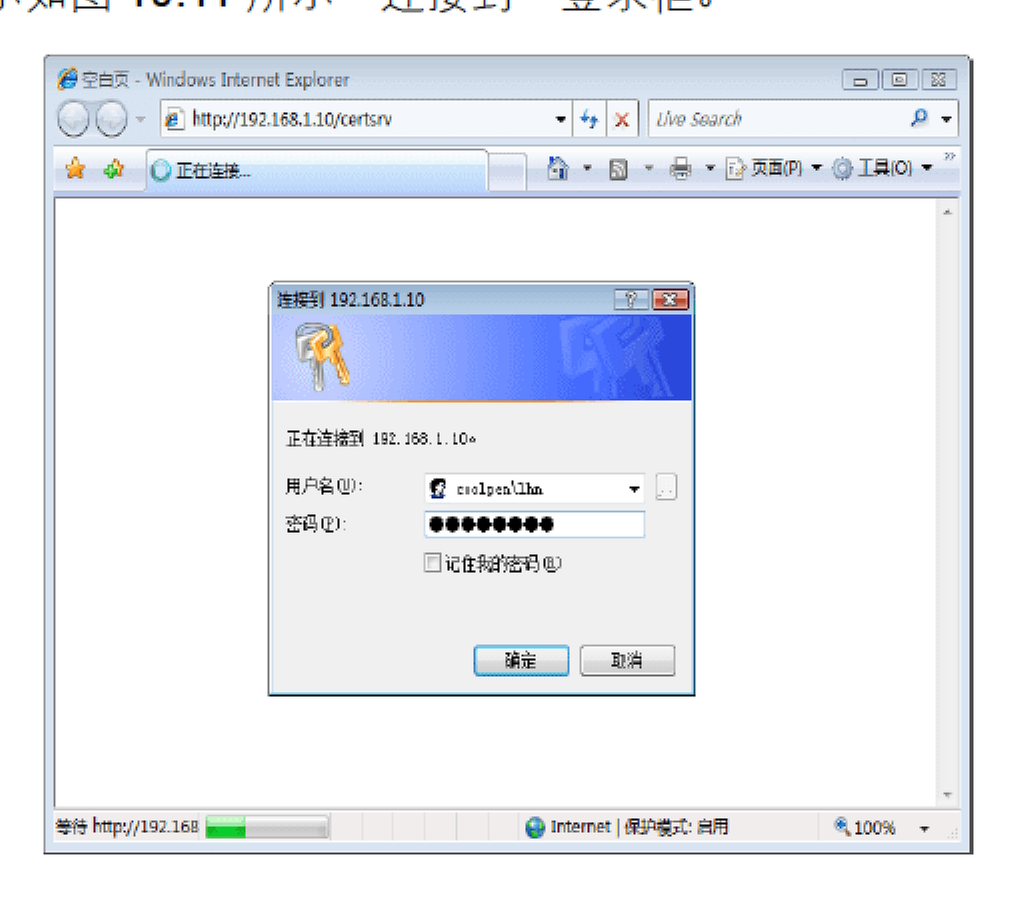


图 10.11　登录框

02 在“用户名”和“密码”文本框中分别输入具有登录证书服务器权限的用户名和密码，单击“确定”按钮，显示如图 10.12 所示“Active Directory 证书服务”窗口。



图 10.12　“Active Directory 证书服务”窗口

03 单击“下载 CA 证书、证书链或 CRL”链接，显示“下载 CA 证书、证书链或 CRL”窗口，用来下载证书或证书链。单击“下载 CA 证书”超级链接，显示如图 10.13 所示“文件下载”对话框。单击“保存”按钮，将该证书保存到本地计算机上。

04 证书下载完成以后，在 Windows 资源管理器中选择所下载的证书文件，右击并选择快捷菜单中的“安装证书”选项，运行“证书导入向导”，单击“下一步”按钮，显示“证书存储”对话框，用来选择保存证书的系统区域。选择“将所有的证书放入下列存储”单选按钮，并单击“浏览”按钮，显示“选择证书存储”对话框，选择“受信任的根证书颁发机构”选项，然后单击“确定”按钮，如图 10.14 所示。

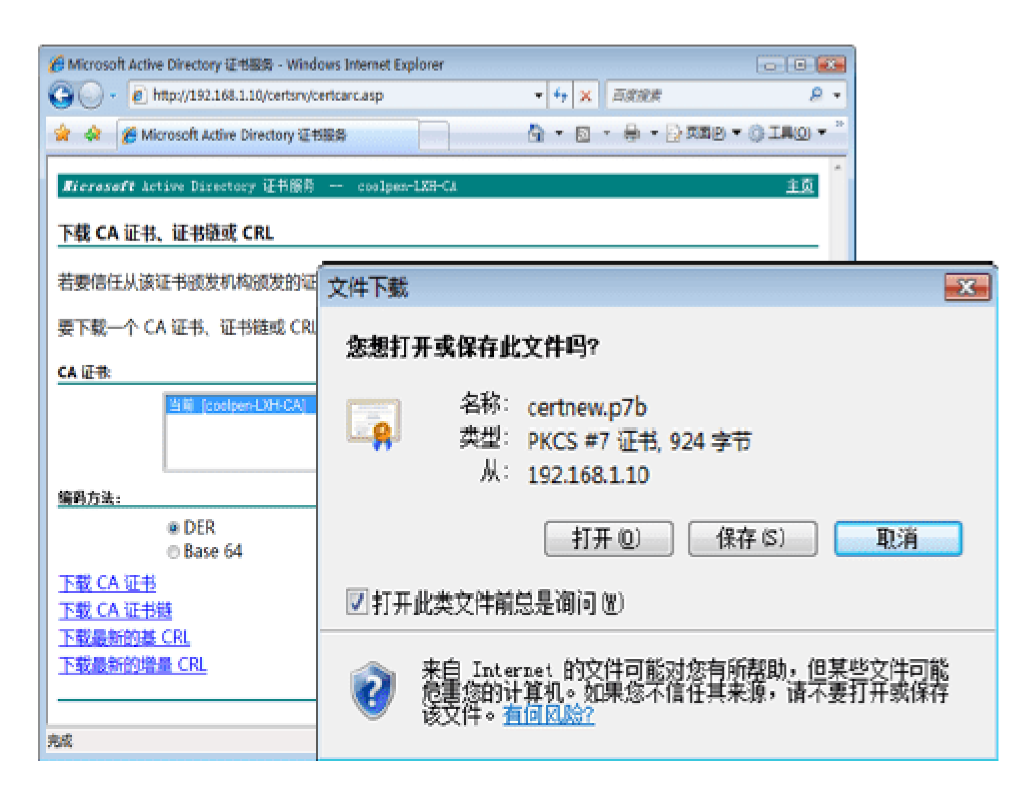


图 10.13　下载证书

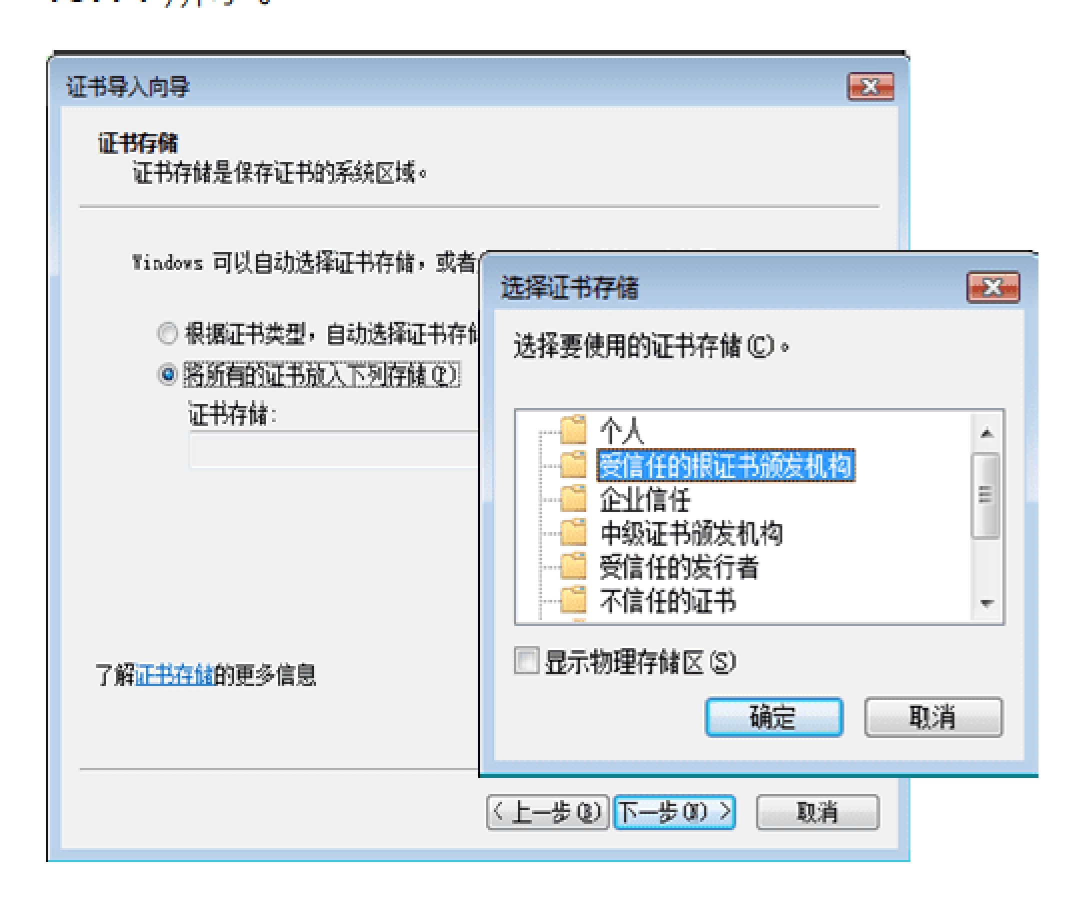


图 10.14　存储证书

05 依次单击“确定”和“下一步”按钮，显示“正在完成证书导入向导”对话框。单击“完成”按钮，显示如图 10.15 所示“安全性警告”对话框，要求确认是否安装此证书。单击“是”按钮，提示证书导入成功。此时，就可以颁发并安装证书了。

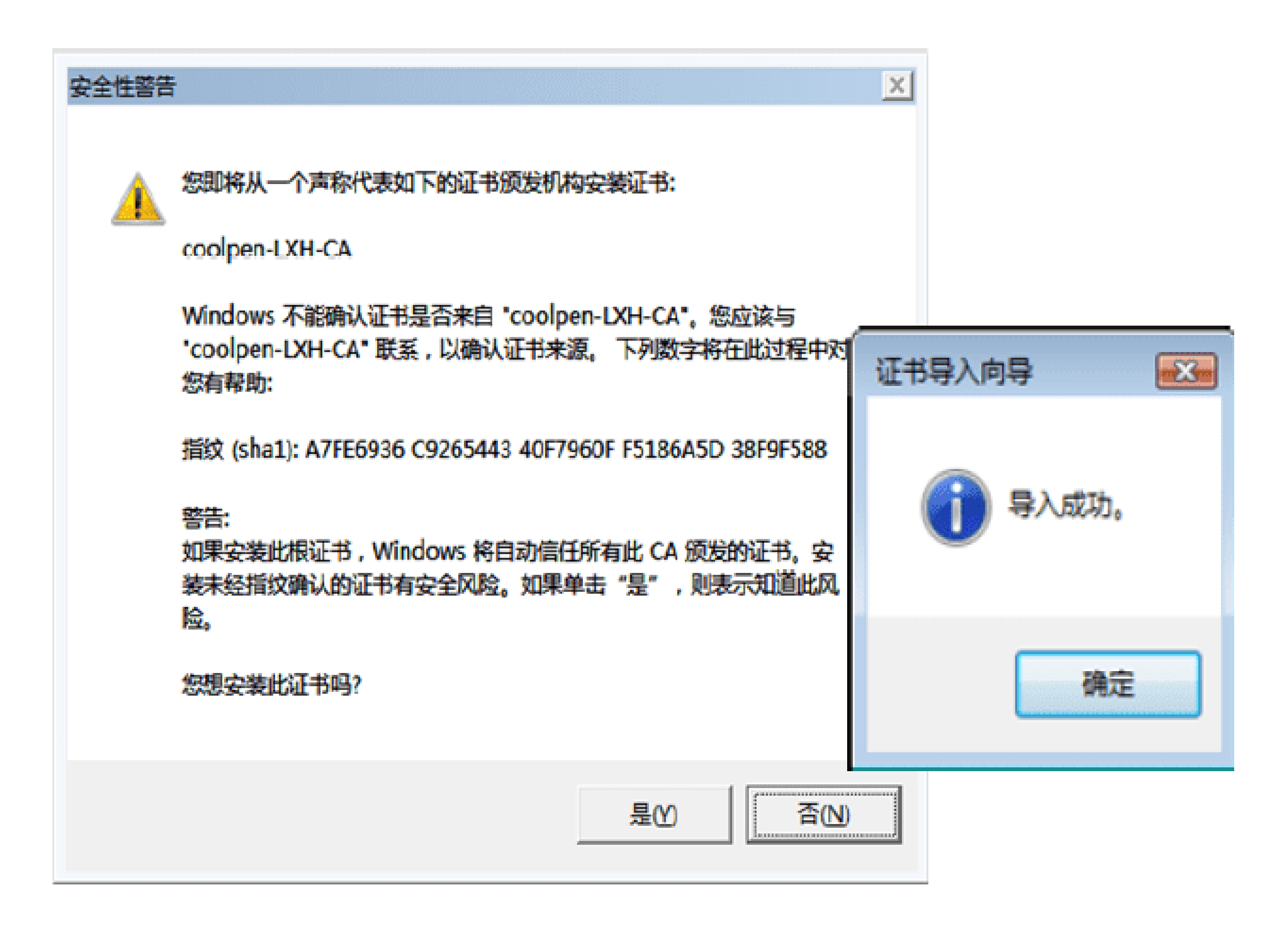


图 10.15 “安全性警告”对话框

3. 申请证书

使用过程配置 Active Directory（R）证书服务（AD CS）用作注册到域成员客户端计算机的计算机证书基础的证书模板。完成此过程之后，域成员客户端计算机会在刷新组策略时自动注册客户端计算机证书。若要刷新组策略，请重新启动客户端计算机，或者在命令提示符下运行 gpupdate 命令。

登录到“Active Directory 证书服务”窗口，在“欢迎使用”窗口中单击“申请证书”超链接，显示“申请一个证书”窗口。单击“用户证书”链接，显示“用户证书—识别信息”窗口。单击“提交”按钮，即可向证书服务器申请证书，完成后显示“证书已颁发”窗口，提示所申请的证书已颁发，如图 10.16 所示。单击“安装此证书”超链接，显示“证书已安装”窗口，即表示证书已经安装。

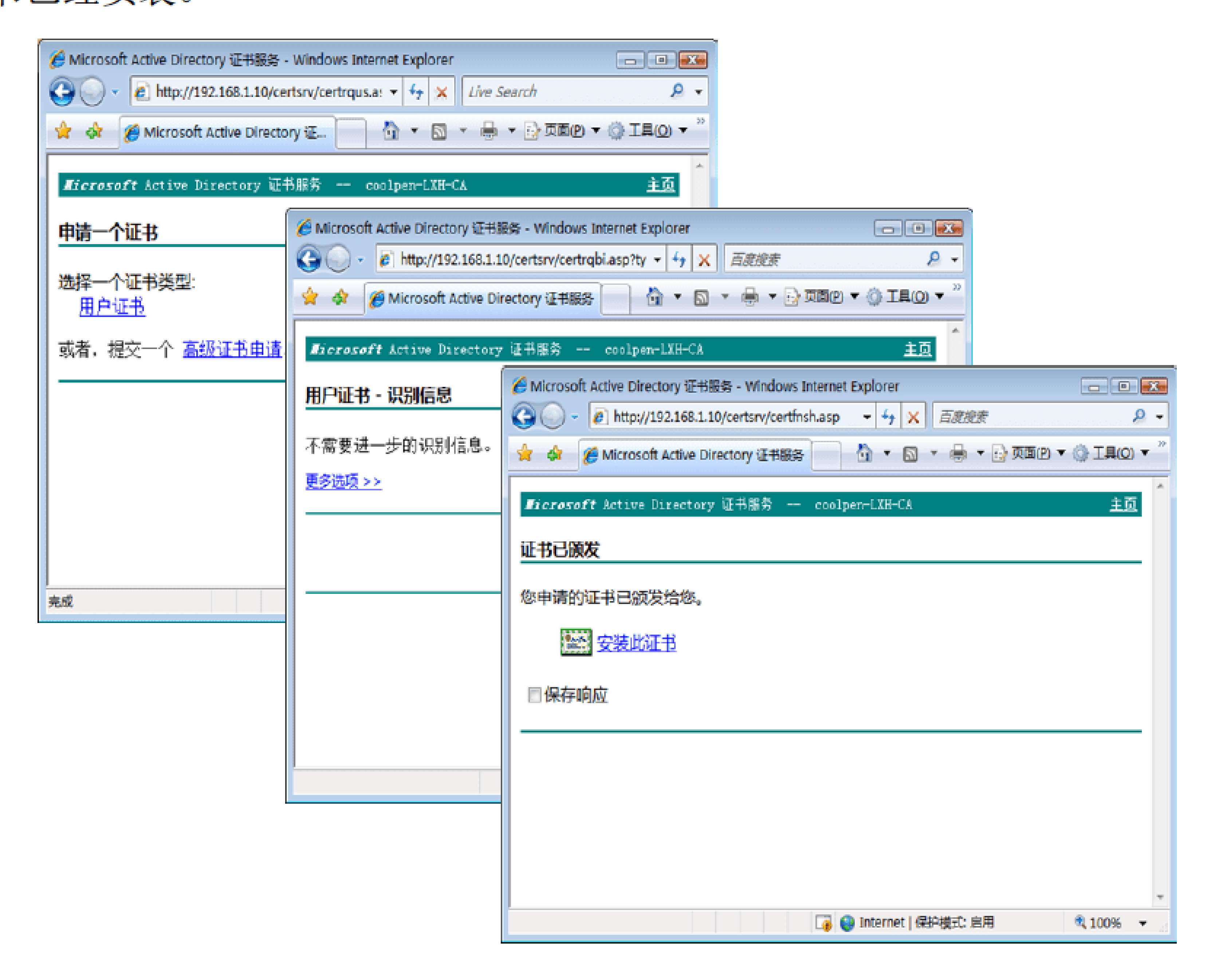


图 10.16 申请和安装证书



10.3.2　使用“证书申请向导”申请证书

要使用“证书申请向导”向企业根 CA 申请证书，客户端计算机必须先加入域，并且使用域用户登录到域。这里以 Windows Vista 为例，介绍如何申请证书。

01　使用域用户帐户登录到 Windows Vista 系统。打开“开始”菜单，在“开始搜索”文本框中输入 mmc 命令，回车，打开“控制台 1”窗口。单击“文件”菜单中的“添加/删除管理单元”选项，显示“添加或删除管理单元”对话框。在“可用的管理单元”列表框中选择“证书”选项，单击“添加”按钮，添加到右侧“所选管理单元”列表框中，如图 10.17 所示。

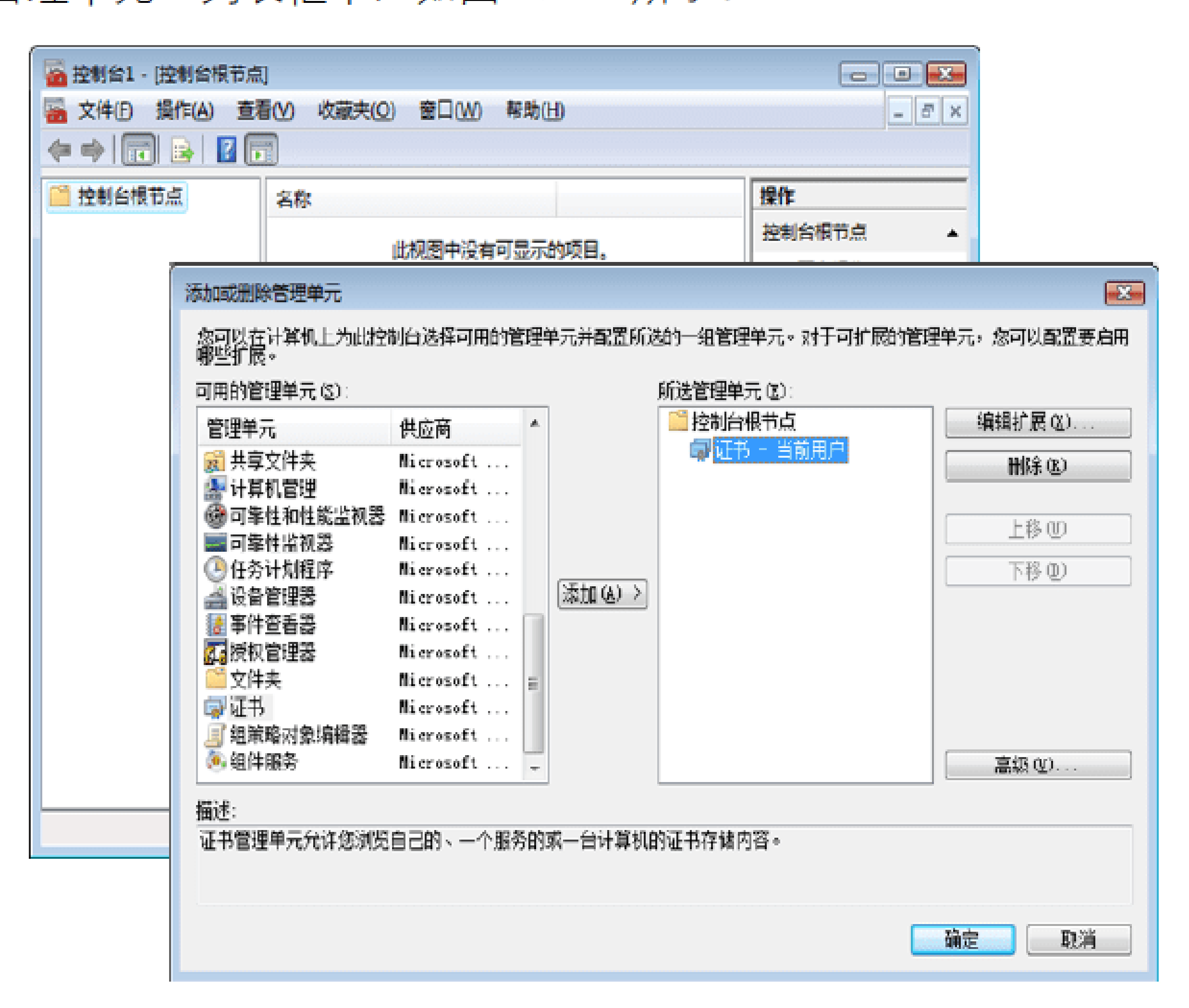


图 10.17　添加证书到所选管理单元

02　单击“确定”按钮，将证书管理单元添加到控制台中。依次展开“证书 － 当前用户”，选择“个人”，右击并选择快捷菜单中的“所有任务”→“申请新证书”命令，启动“证书注册”向导。单击“下一步”按钮，显示如图 10.18 所示“申请证书”对话框，在列表框中选择欲申请的证书类型，单击“详细信息”按钮，可以查看该证书的详细信息。默认情况下，只列出了可用的证书模板。

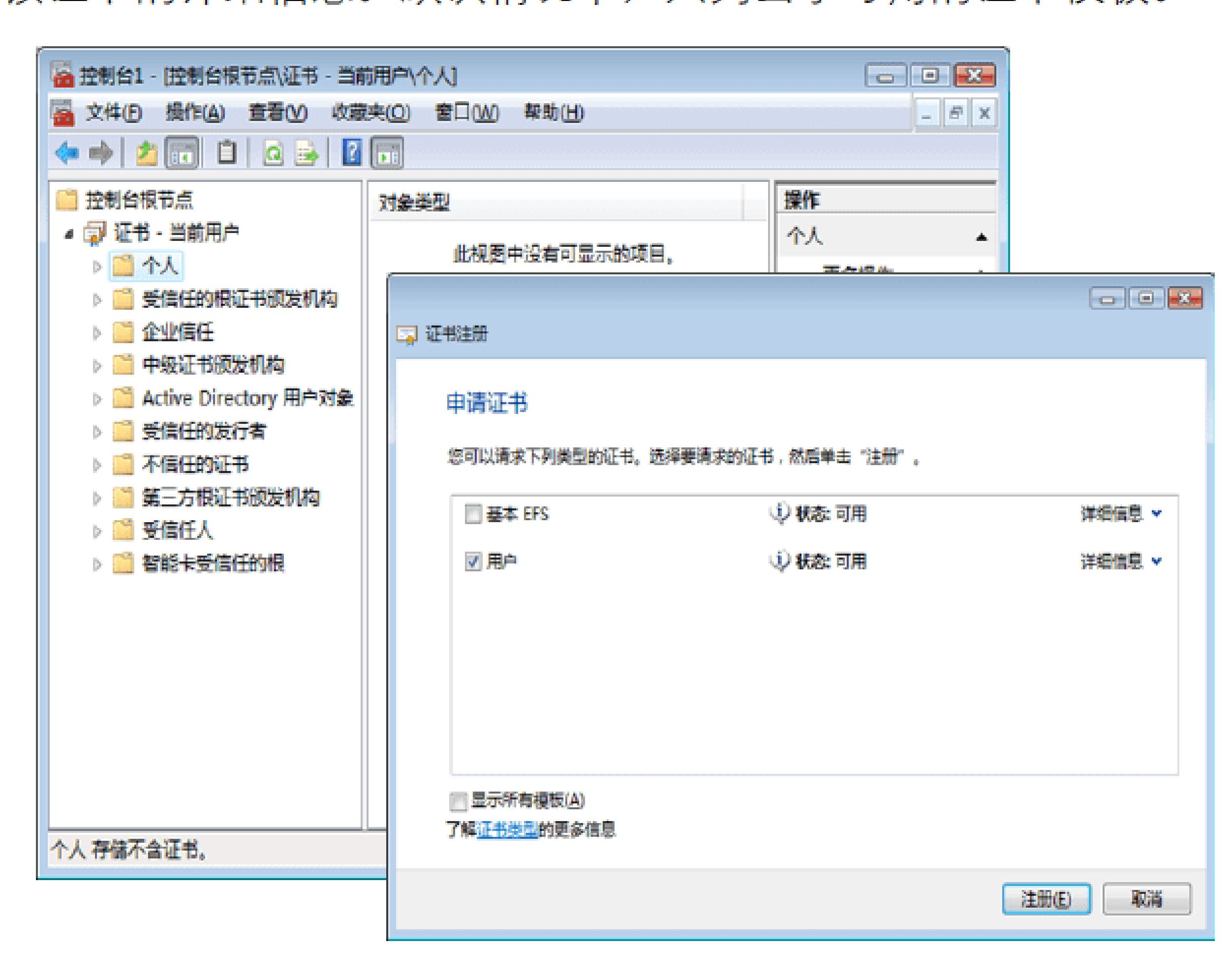


图 10.18　申请证书

03 单击“注册”按钮，系统会向证书服务器申请注册并自动安装，成功完成后单击“完成”按钮关闭证书注册向导，并返回控制台。依次展开“证书 - 当前用户”→“个人”→“证书”选项，即可看到已注册成功的证书。

至此，证书注册完成。返回 Windows Server 2008 证书服务器，依次单击“开始”→“管理工具”→“Certification Authority”命令，打开“证书颁发机构”窗口。选择“颁发的证书”，即可看到所有已颁发的证书，如图 10.19 所示。

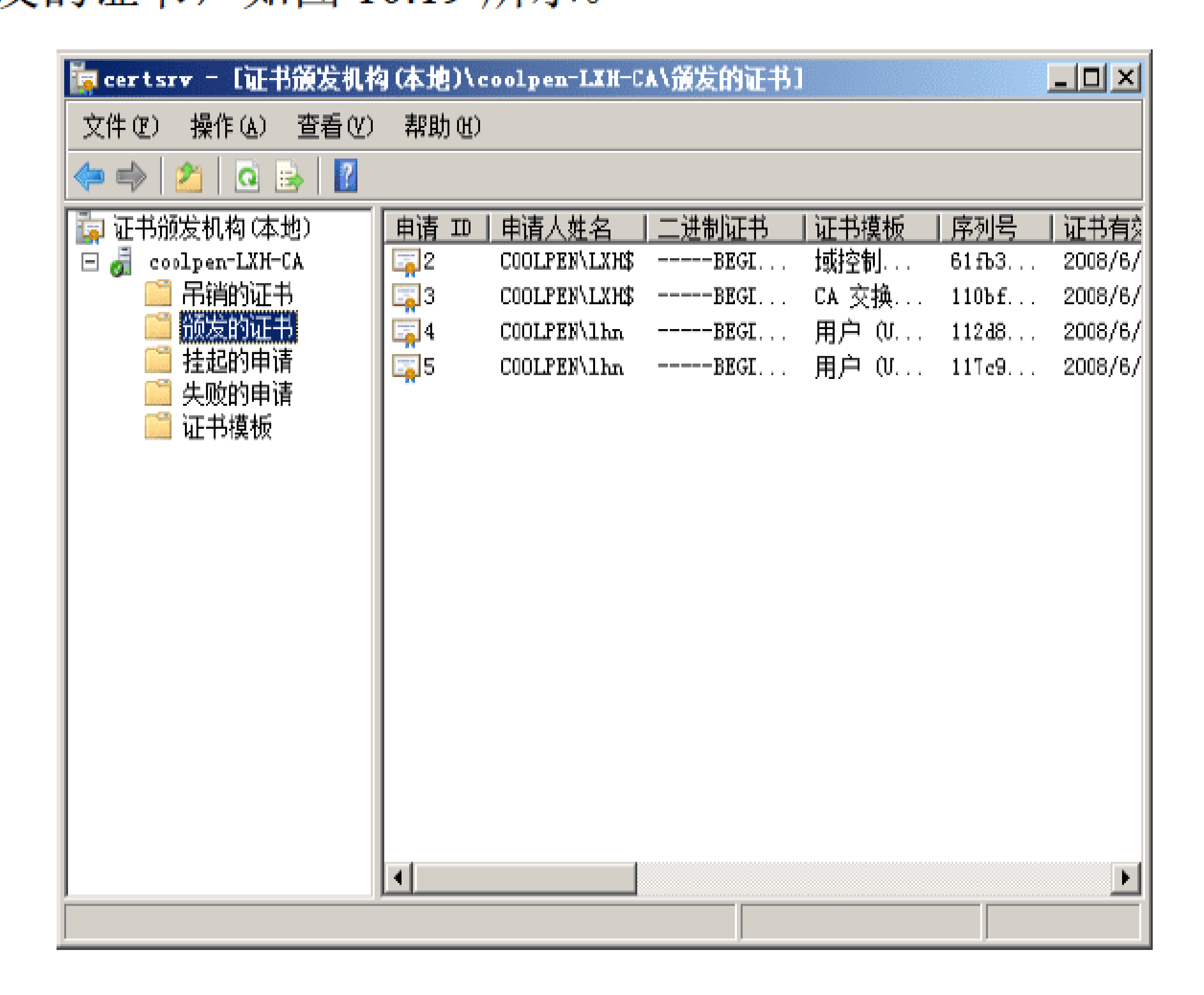


图 10.19 颁发的证书

10.3.3 导出与导入证书

为了防止因意外故障或者重新安装系统而造成证书损坏或丢失，用户可以事先将证书导出以进行备份，而当需要还原时，只需将证书导入即可，不必再重新申请。

1. 导出证书

在 Windows Server 2008 中对证书进行导出，其具体操作步骤如下。

01 在客户端计算机上运行“mmc”命令，打开控制台窗口，添加“证书”管理单元。展开要备份的证书所在的位置，例如“证书 - 当前用户”→“个人”→“证书”选项，选择欲导出的证书，右击并依次选择快捷菜单中的“所有任务”→“导出”命令，运行“证书导出向导”。单击“下一步”按钮，显示如图 10.20 所示“导出私钥”对话框，选择是否要导出私钥。



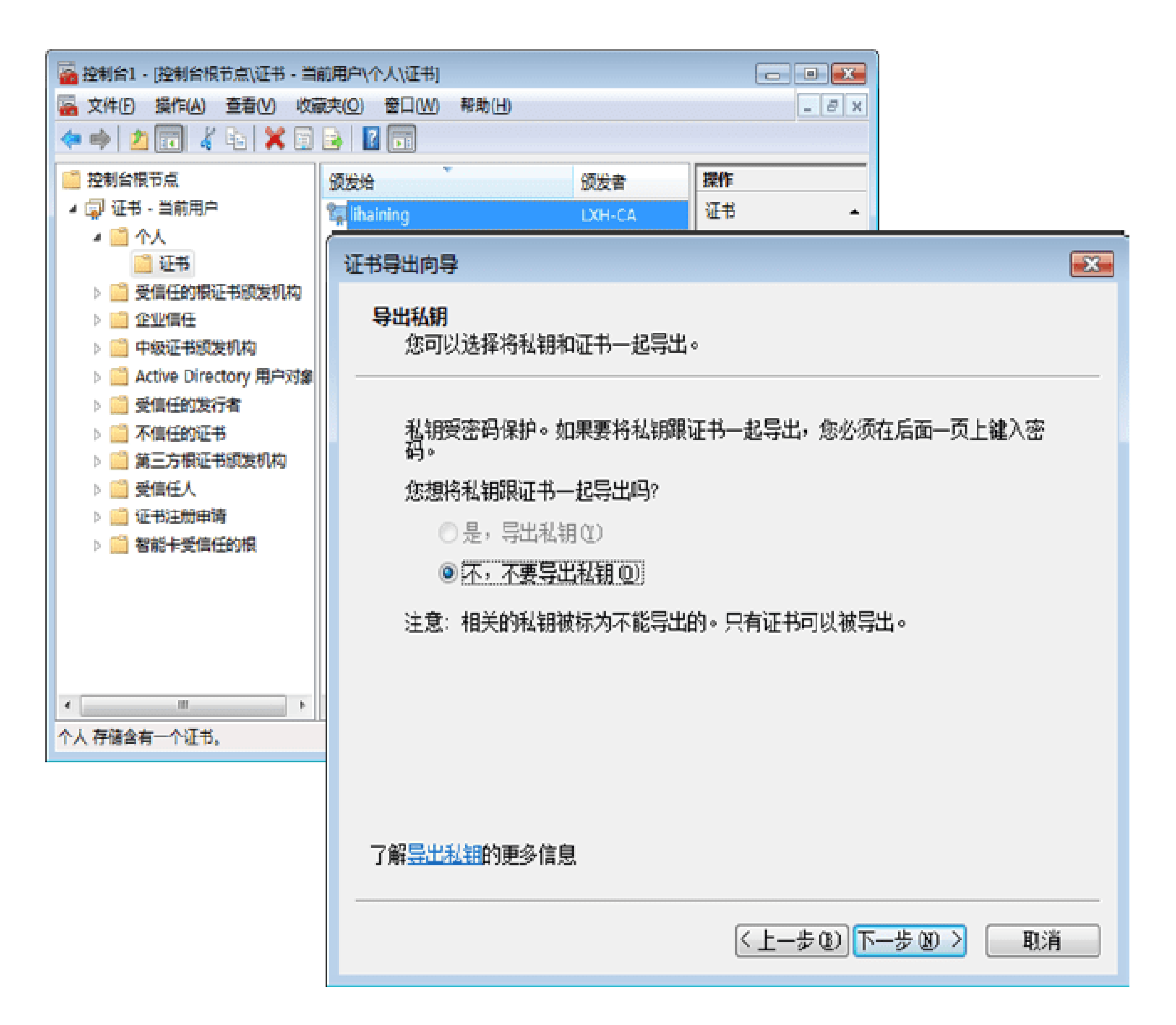


图 10.20　导出私钥

02 依次单击“下一步”按钮，设置导出证书文件格式和保存路径，如图 10.21 所示。完成设置后在“正在完成证书导出向导”对话框中，单击“完成”按钮，即可提示用户“导出”成功。至此，导出证书完毕。

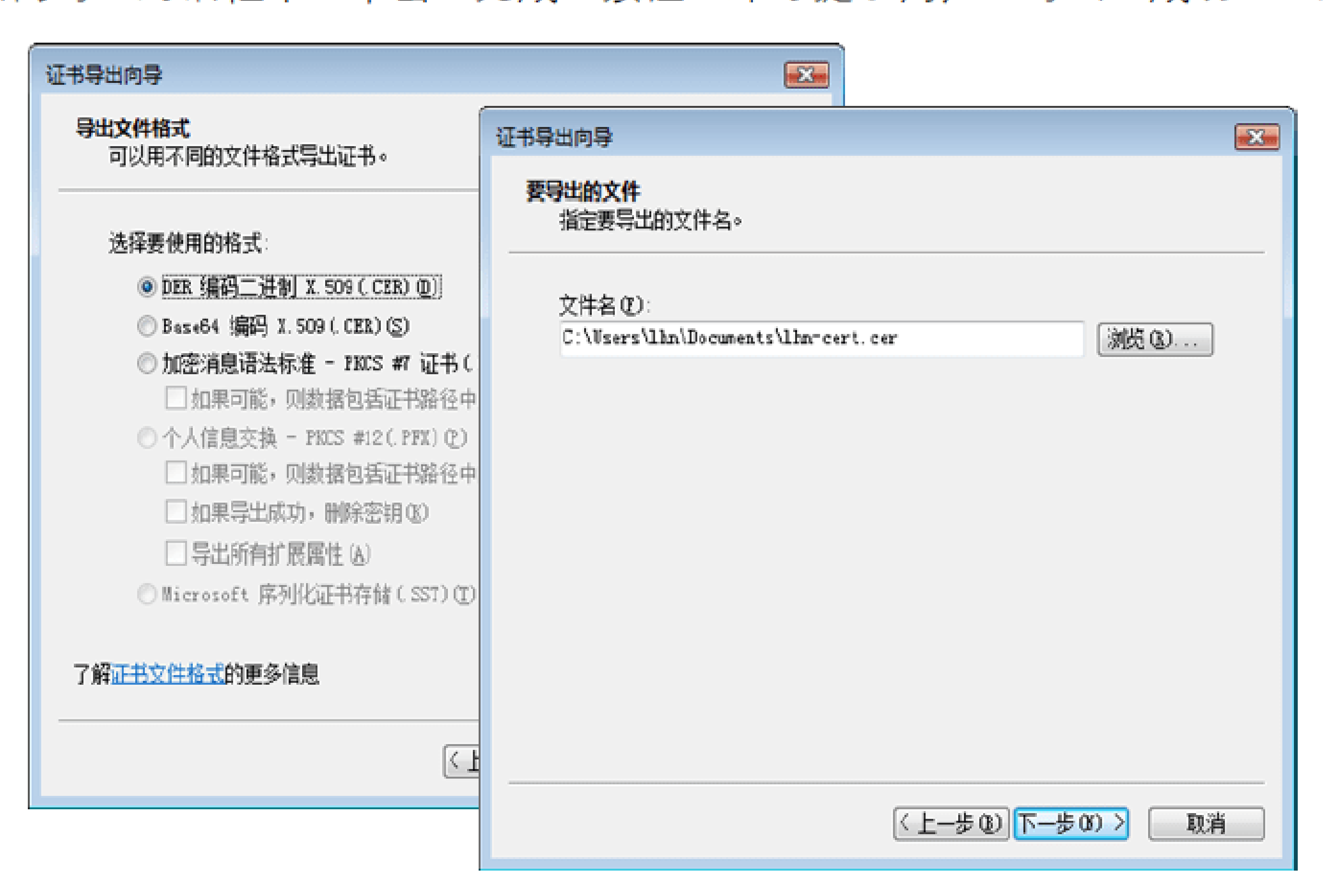


图 10.21　设置导出证书文件格式和保存路径

2. 导入证书

打开“控制台”窗口，添加“证书”管理单元，展开“个人”，右击“证书”并依次选择快捷菜单中的“所有任务”→“导入”命令，运行“证书导入向导”。单击“下一步”按钮，显示“要导入的文件”对话框，单击“浏览”按钮，选择以前导出的证书文件。单击“下一步”按钮，选择证书的存储位置，如图 10.22 所示。依次单击“下一步”按钮，直至完成“证书导入向导”即可。

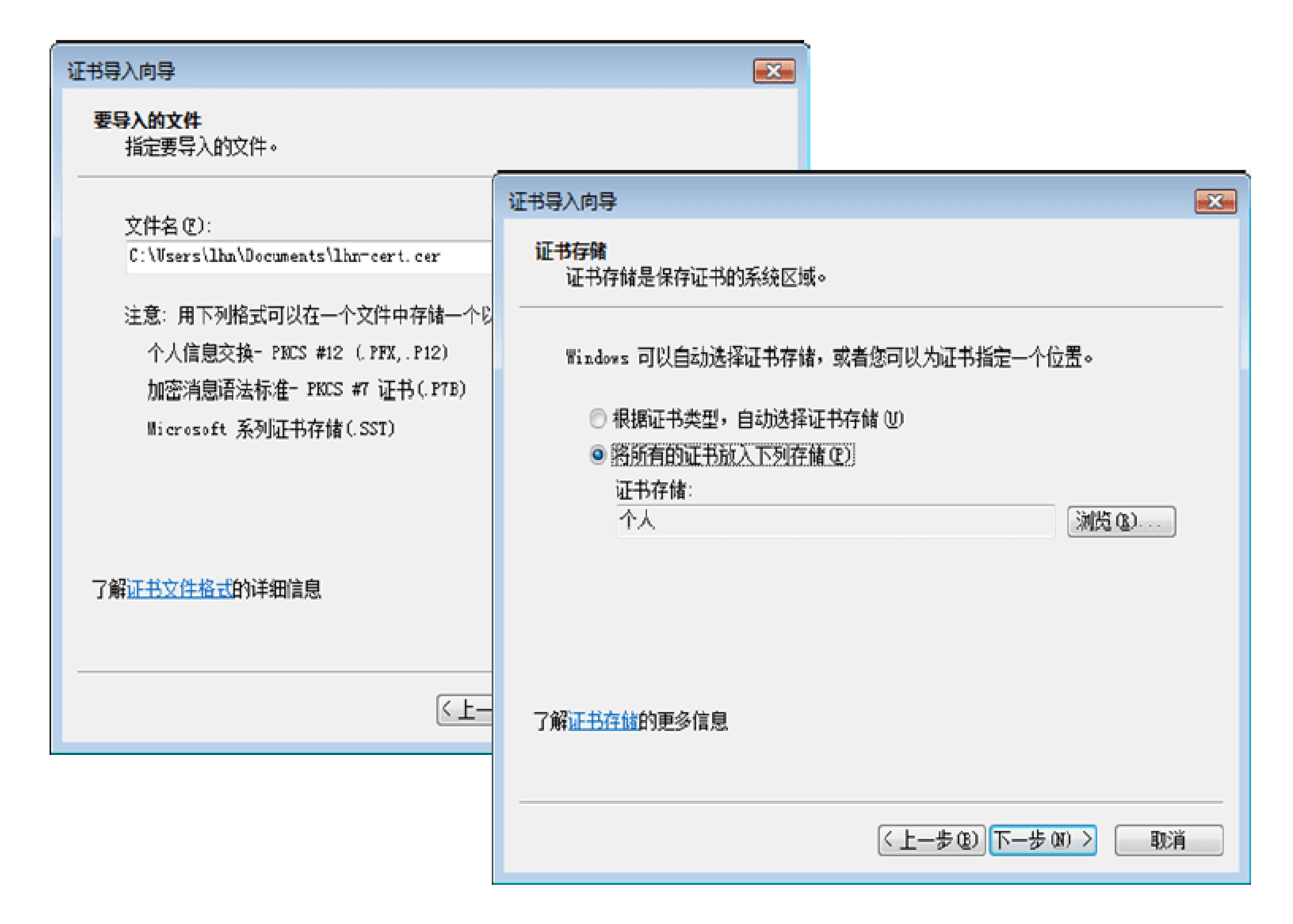


图 10.22　导入证书

10.4　独立证书服务器的应用

独立证书服务器由于没有加入域，因此，不能使用“证书申请向导”来申请证书，只能以 Web 方式向证书服务器申请证书。为了证书服务的安全，当用户申请证书后并不会立即安装，必须由管理员颁发后才能使用。

10.4.1　申请证书

在向服务器申请证书时，必须先做好如下准备工作：

- 在 IE 浏览器的安全设置中，将“对未标记为可安全执行脚本的 ActiveX 控件初始化并执行脚本（不安全）”和“允许运行以前未使用的 ActiveX 控件而不提示”均选择为“启用（不安全）”选项；
- 下载 CA 证书并导入到客户端计算机上，使其信任证书颁发机构。

向独立服务器申请证书的操作步骤如下。

01 在 IE 浏览器中打开申请独立根证书的地址，格式为 http://证书服务器 IP 地址/certsrv，显示如图 10.23 所示证书服务主页。

02 单击“申请证书”超级链接，显示如图 10.24 所示“申请一个证书”窗口。可以直接申请 Web 浏览器证书或电子邮件证书，也可以提交高级证书申请。





图 10.23　证书服务主页

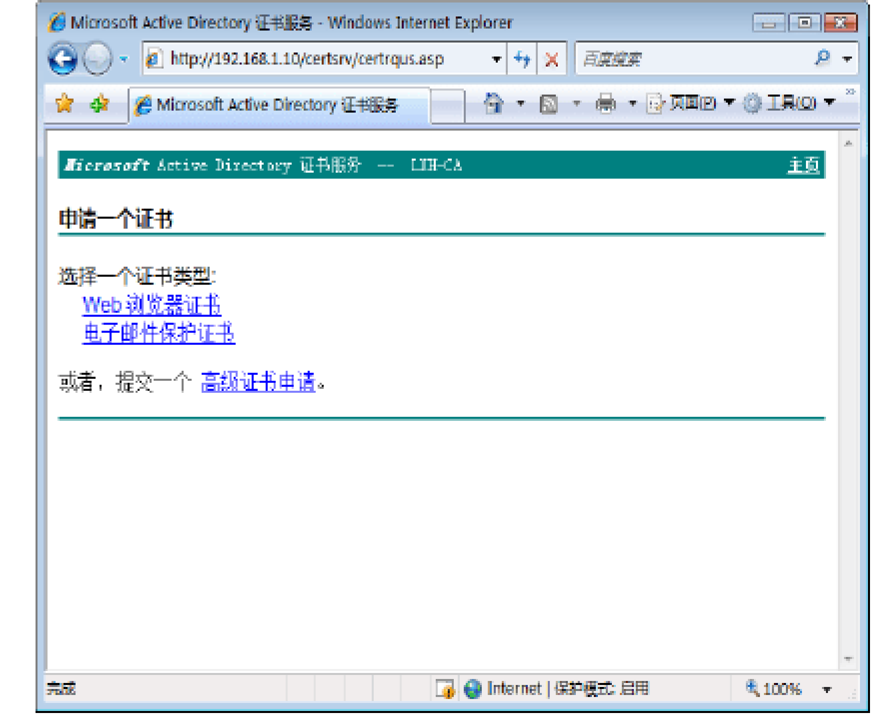


图 10.24　“申请一个证书”窗口

提示　如果要申请其他类型的证书，可单击“高级证书申请”链接。同时，还可以选择不同的密钥类型，如图 10.25 所示。

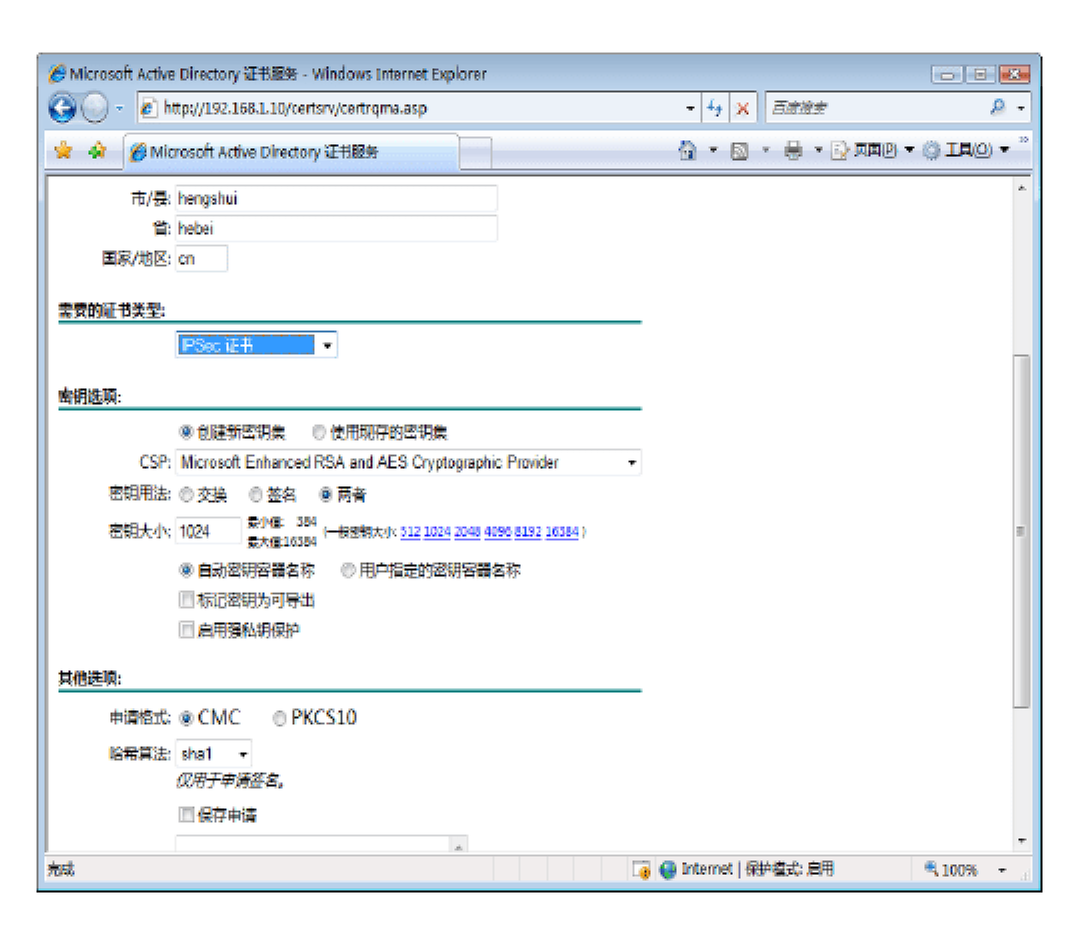


图 10.25　高级证书申请

03 这里以申请电子邮件保护证书为例。单击“电子邮件保护证书”超级链接，显示如图 10.26 所示“电子邮件保护证书　识别信息”窗口，输入电子邮件保护证书的识别信息即可。

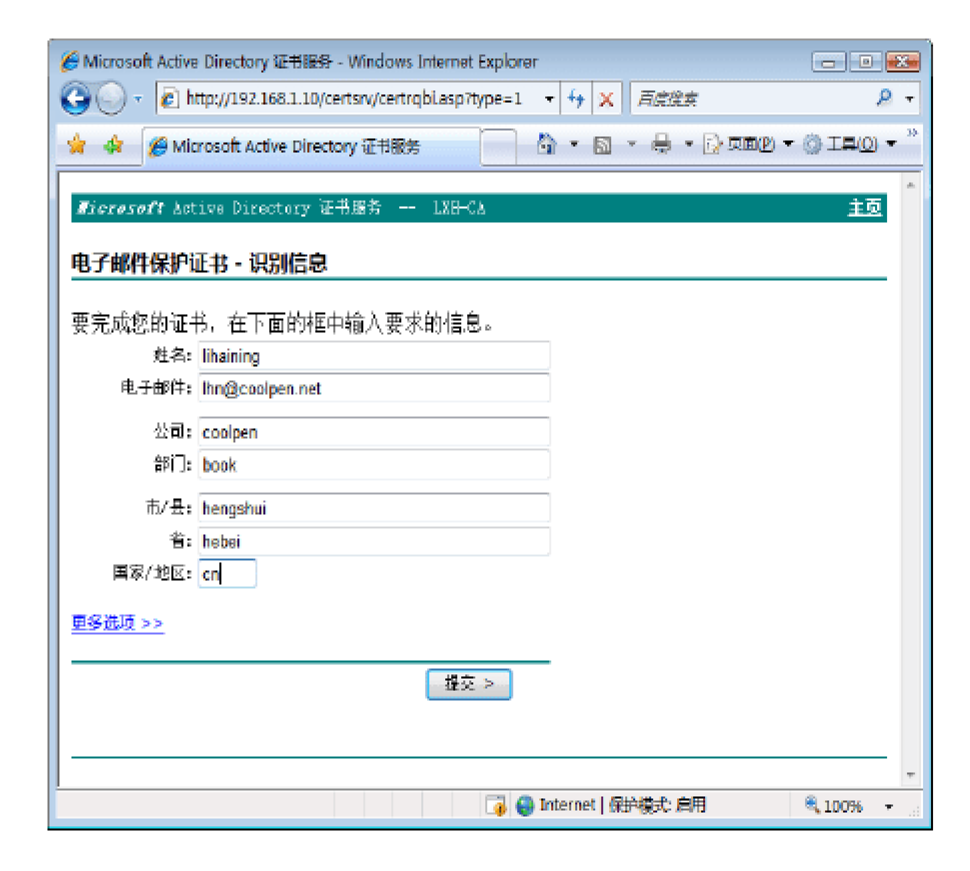


图 10.26　申请电子邮件证书

提示 如果不想使用默认的密钥类型，可以单击“更多选项”链接，显示如图 10.27 所示，在“选择一个加密服务提供程序”下拉列表中可选择不同的密钥程序。



图 10.27 选择不同密钥类型

04 单击“提交”按钮，开始向证书服务器发送请求，显示如图 10.28 所示“证书正在挂起”窗口。提示已发出申请，但必须等待管理员来颁发证书。

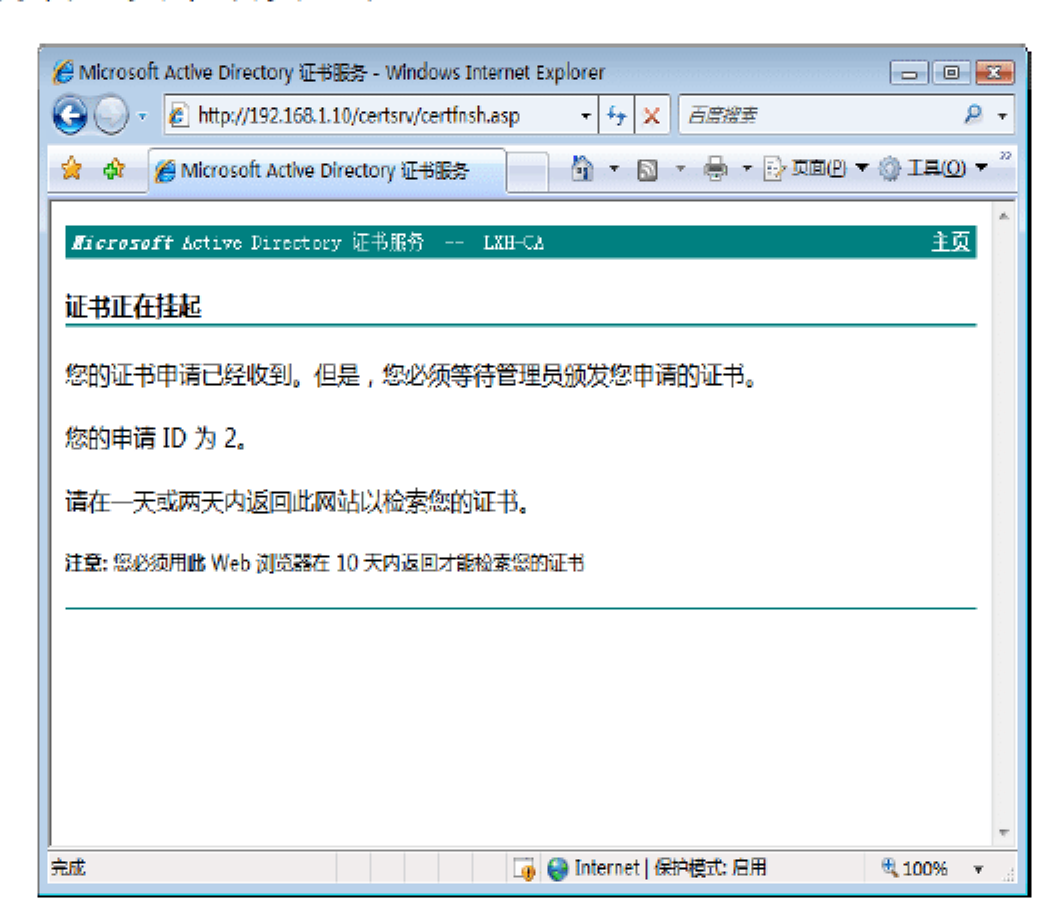


图 10.28 “证书正在挂起”窗口

10.4.2 颁发证书

此时，在 Windows Server 2008 服务器上，需要由管理员查看证书申请，并颁发证书。

01 登录到证书服务器，依次单击“开始”→“管理工具”→“Certification Authority”命令，打开“certsrv”窗口。在左侧栏中选择“挂起的申请”选项，即可显示所有提交的证书申请，如图 10.29 所示。

02 选择欲颁发的证书，右击并依次选择快捷菜单中的“所有任务”→“颁发”命令，即可颁发该证书。同时，已颁发的证书将会自动转到“颁发的证书”窗口中，如图 10.30 所示。



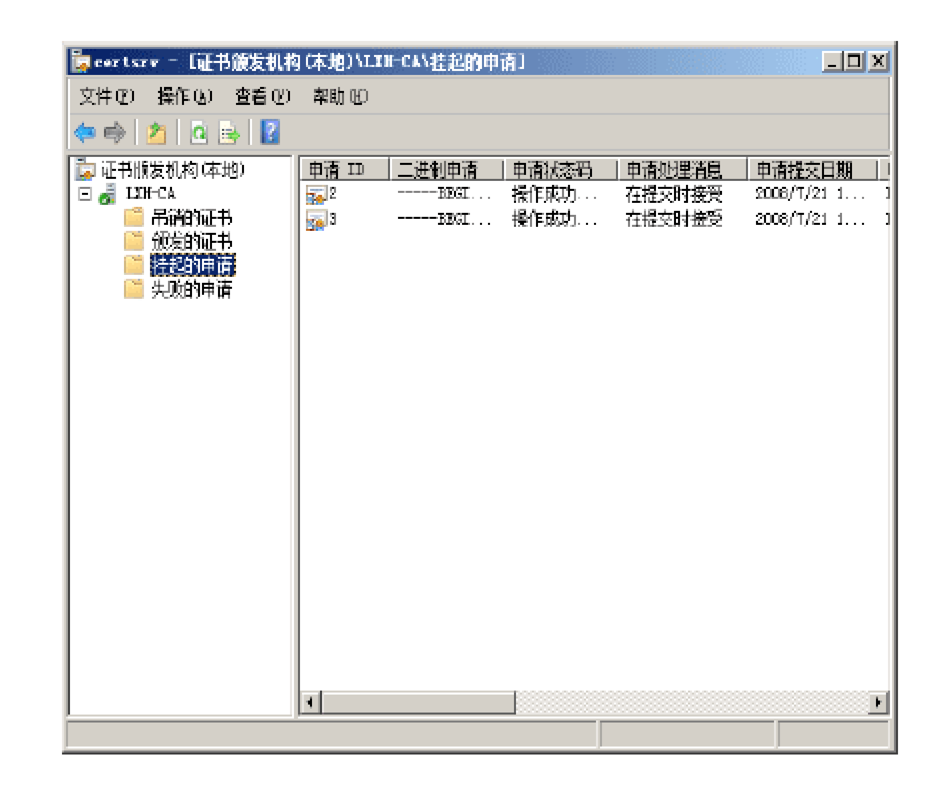


图 10.29　挂起的申请

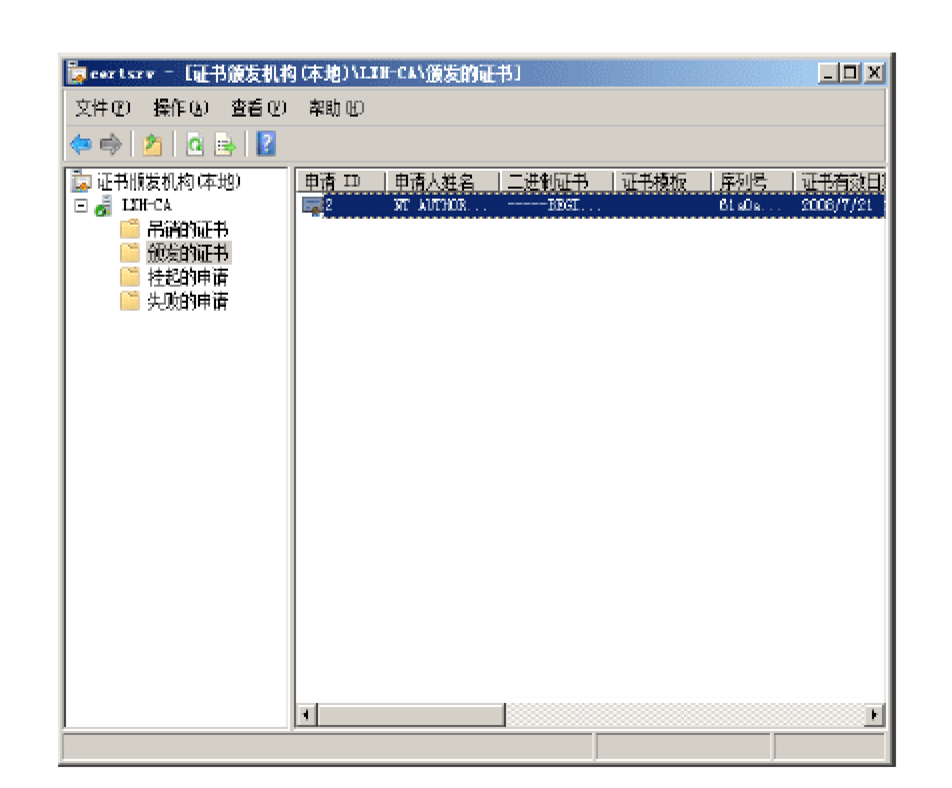


图 10.30　颁发的证书

此时，证书颁发完成，在客户端计算机上就可以安装或下载证书了。

10.4.3　在客户端安装证书

在客户端计算机上，重新打开证书服务主页，单击“查看挂起的证书申请的状态”链接，显示“查看挂起的证书申请的状态”窗口，列出了曾经申请的证书。单击证书名称，例如“电子邮件保护证书”，显示“证书已颁发”窗口，提示该证书已颁发，可以安装了。单击“安装此证书”链接，显示“证书已安装”窗口，即可将该证书安装在本地计算机上，如图 10.31 所示。

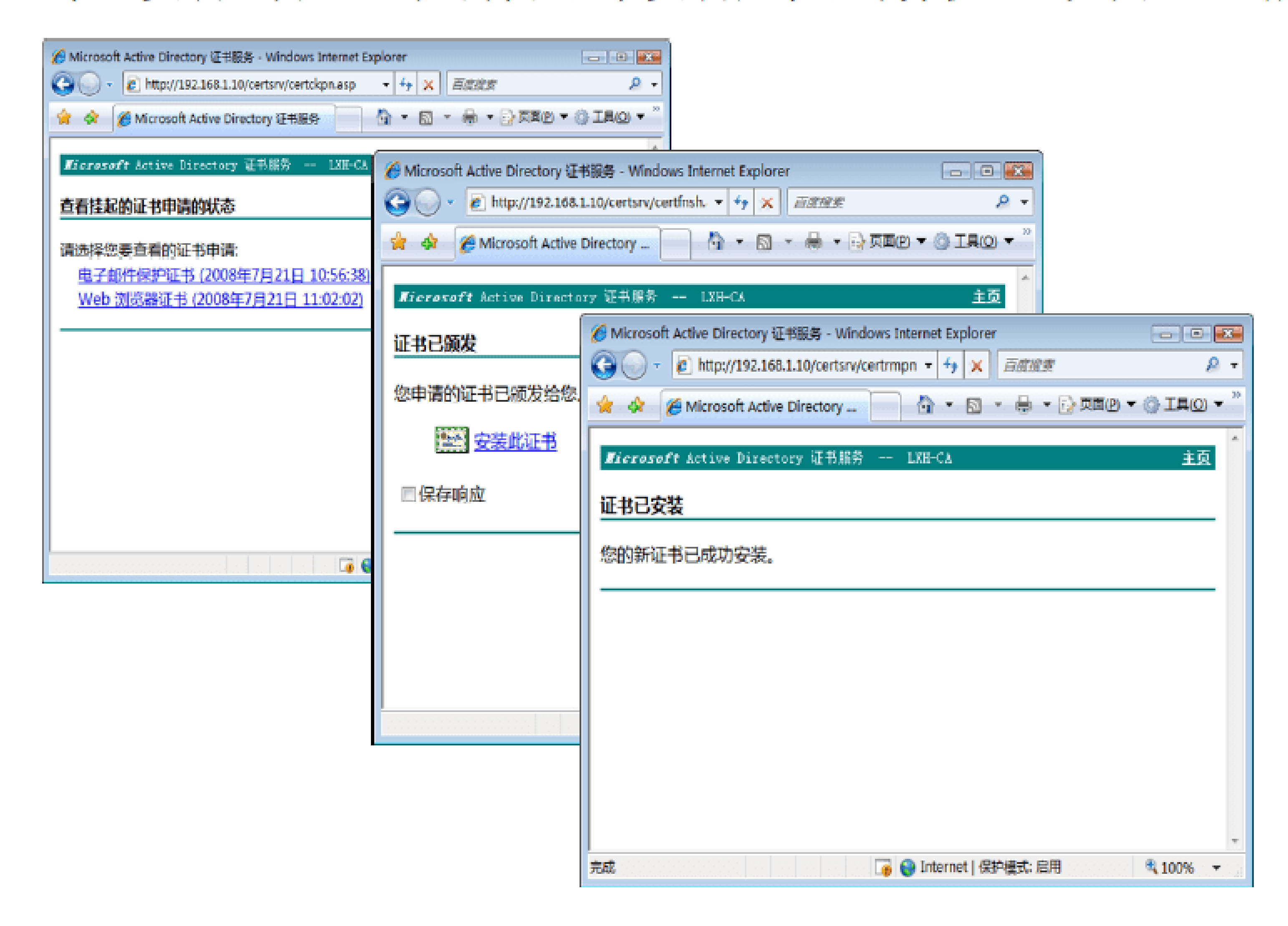


图 10.31　在客户端安装证书

10.5　证书服务器的备份与还原

为了防止证书服务器因意外故障或证书被误删而导致证书丢失，对用户的使用造成损失，

管理员和用户都应定期备份证书服务器中的证书，以便在证书丢失或损坏时能够及时还原，可继续使用而不必再重新申请。

10.5.1 证书的备份

把服务器证书从服务器备份出来，以便服务器硬件或软件系统坏了需要重装系统时可以重装服务器证书。

01 以管理员用户身份登录到证书服务器，打开“证书颁发机构”窗口，右击证书服务器名称，依次选择快捷菜单中的“所有任务”→“备份 CA”命令，运行“证书颁发机构备份向导”。单击“下一步”按钮，显示如图 10.32 所示“要备份的项目”对话框，在“选择要备份的项目”选项区域中，选择要备份的组件，如“私钥和 CA 证书”、“证书数据库和证书数据库日志”；在“备份到这个位置”文本框中输入备份证书的保存路径，或单击“浏览”按钮选择。

02 单击“下一步”按钮，显示如图 10.33 所示“选择密码”对话框。为安全起见，可在“密码”文本框中设置访问 CA 证书文件的密钥，防止被其他人访问。

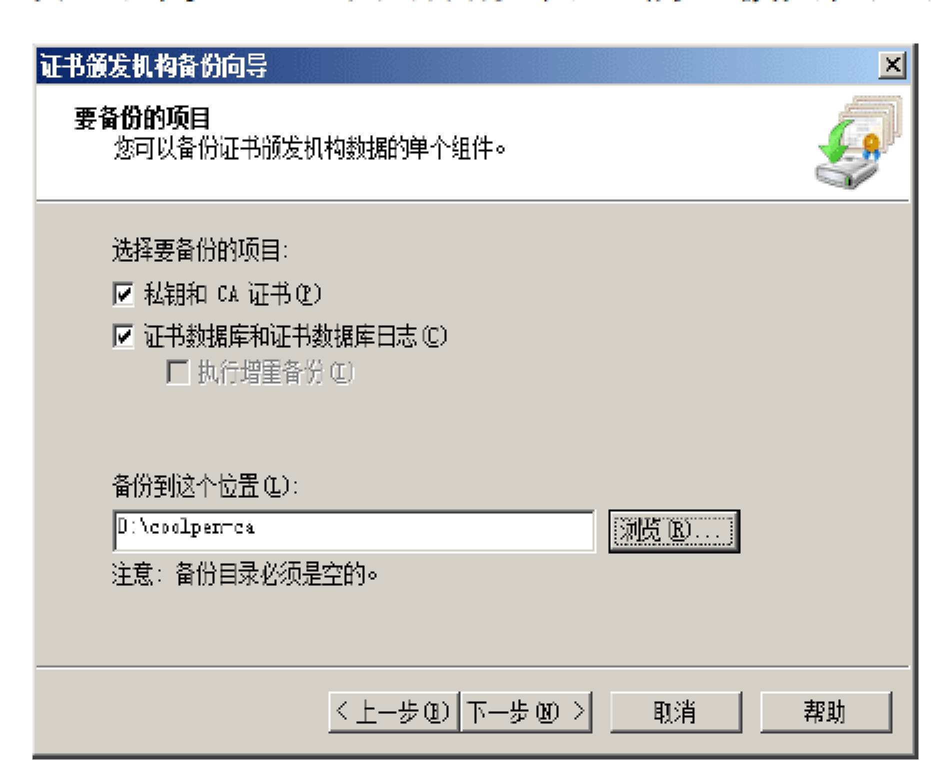


图 10.32 “要备份的项目”对话框

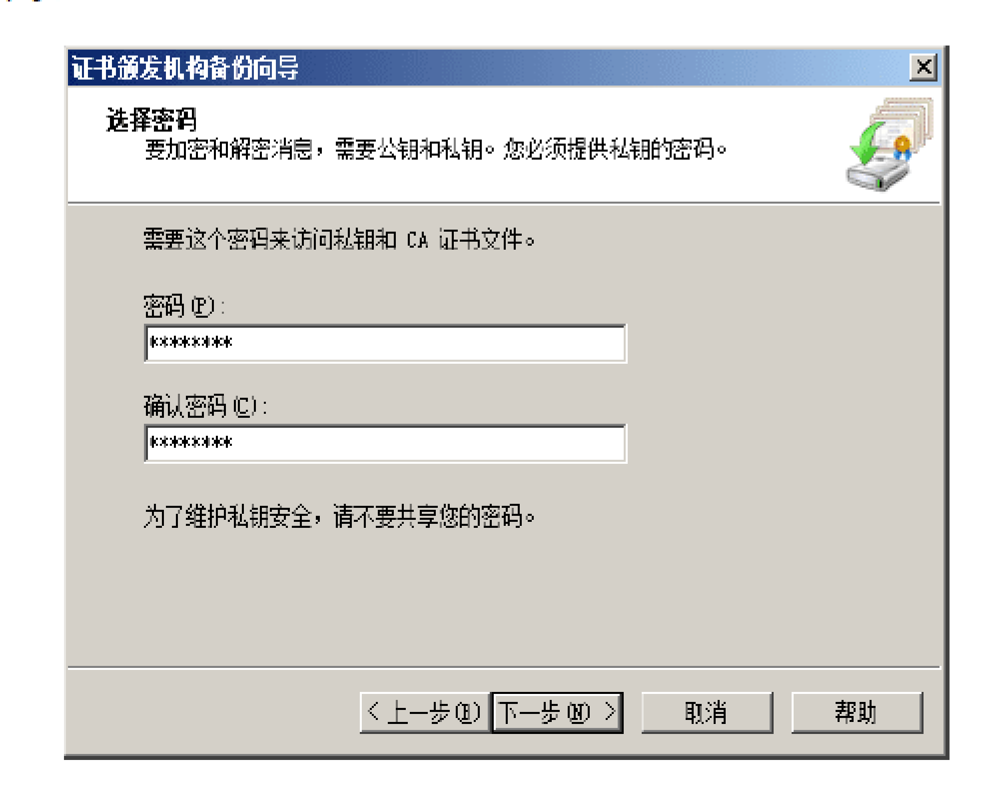


图 10.33 “选择密码”对话框

03 单击“下一步”按钮，显示“正在完成证书颁发机构备份向导”对话框。单击“完成”按钮，即可备份证书。

10.5.2 证书的还原

对服务器证书进行还原操作，以便及时应用证书。

01 在“证书颁发机构”窗口中，右击证书服务器名，依次选择快捷菜单中的“所有任务”→“还原 CA”命令，显示如图 10.34 所示提示框，提示还原证书过程中不能运行 Active Directory 证书服务，需要立即停止证书服务。

02 单击“确定”按钮，停止 Active Directory 证书服务，并启动证书颁发机构还原向导。单击“下一步”按钮，显示如图 10.35 所示“要还原的项目”对话框，在“选择要还原的项目”选项区域中选择要还原的选项，在“从这个位置还原”文本框中输入备份证书所在的路径，或者单击“浏览”按钮选择。



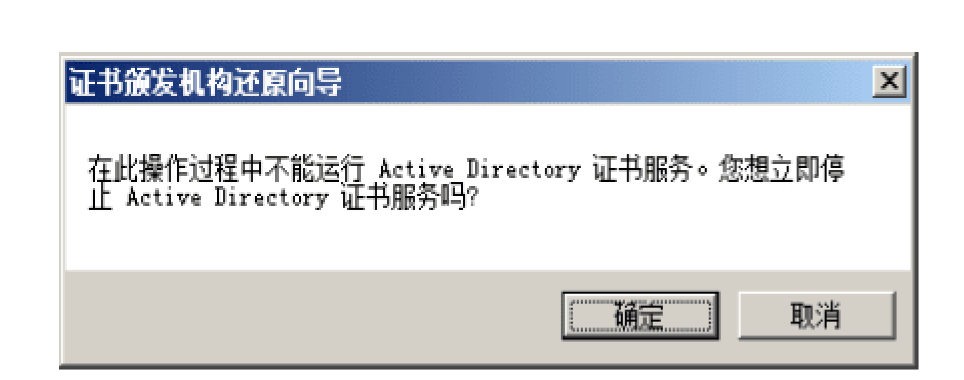


图 10.34　提示框



图 10.35　“要还原的项目”对话框

03 单击“下一步”按钮，显示如图 10.36 所示“提供密码”对话框，在“密码”文本框中输入备份 CA 时设置的密码。

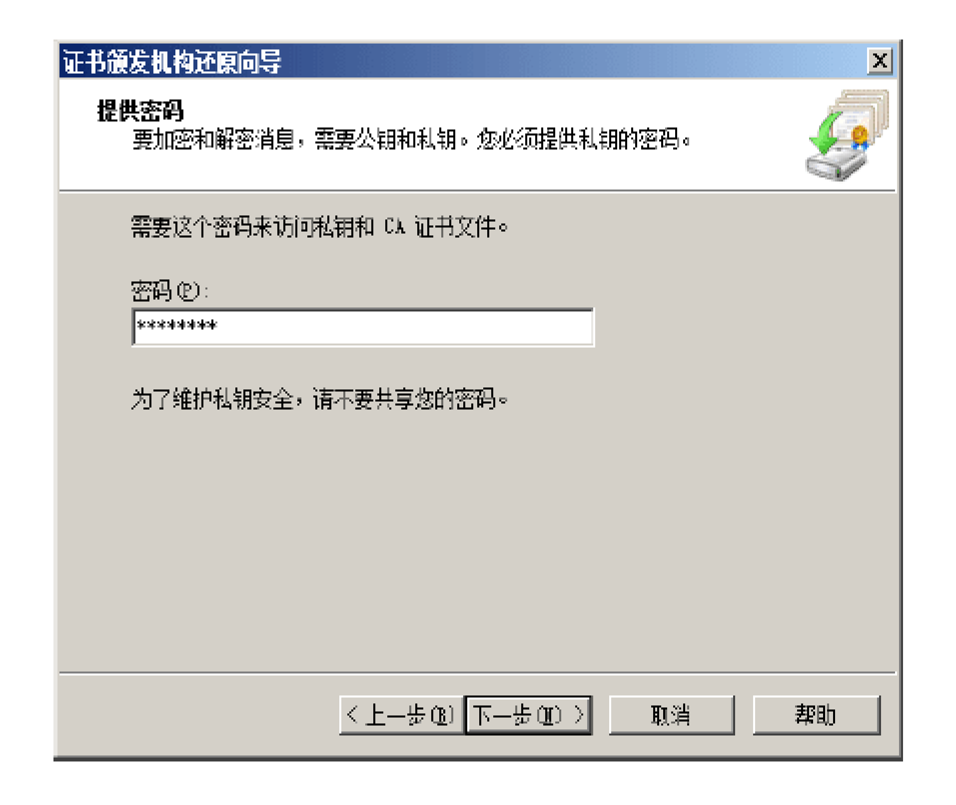


图 10.36　“提供密码”对话框

04 单击“下一步”按钮，显示“证书颁发机构还原向导”对话框。单击“完成”按钮，证书还原成功，显示如图 10.37 所示对话框，提示是否要启动服务。



图 10.37　还原完成

05 单击“是”按钮，启动 Active Directory 证书服务。

10.6　证书服务的管理

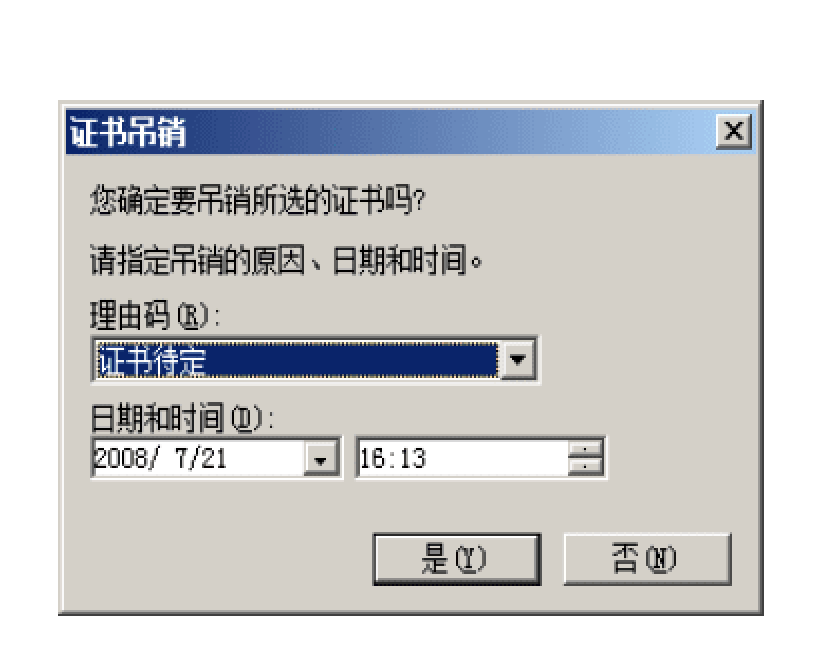
在企业中，人员变动是经常发生的事，当员工离开公司或调到其他部门，该员工原来申请的证书将不再使用，此时，网络管理员就应及时吊销其证书。证书都有一定的有效期限，为了保证在有效期过后仍能继续使用，应及时更新或者续订。

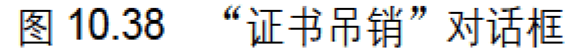
10.6.1　吊销证书

如果某些证书不再使用，即可将其吊销。不过，吊销证书只能在证书服务器上进行，客户机无法吊销证书。

01 登录到证书服务器，打开“证书颁发机构”控制台，在“颁发的证书”窗口中选择欲吊销的证书，右击并依次选择快捷菜单中的“所有任务”→“吊销证书”，显示如图 10.38 所示“证书吊销”对话框，在“理由码”下拉列表中可选择吊销的原因。

02 单击“是”按钮，即可吊销该证书。当证书被吊销以后，将显示在“吊销的证书”窗口中，如图 10.39 所示。




图 10.38 “证书吊销”对话框

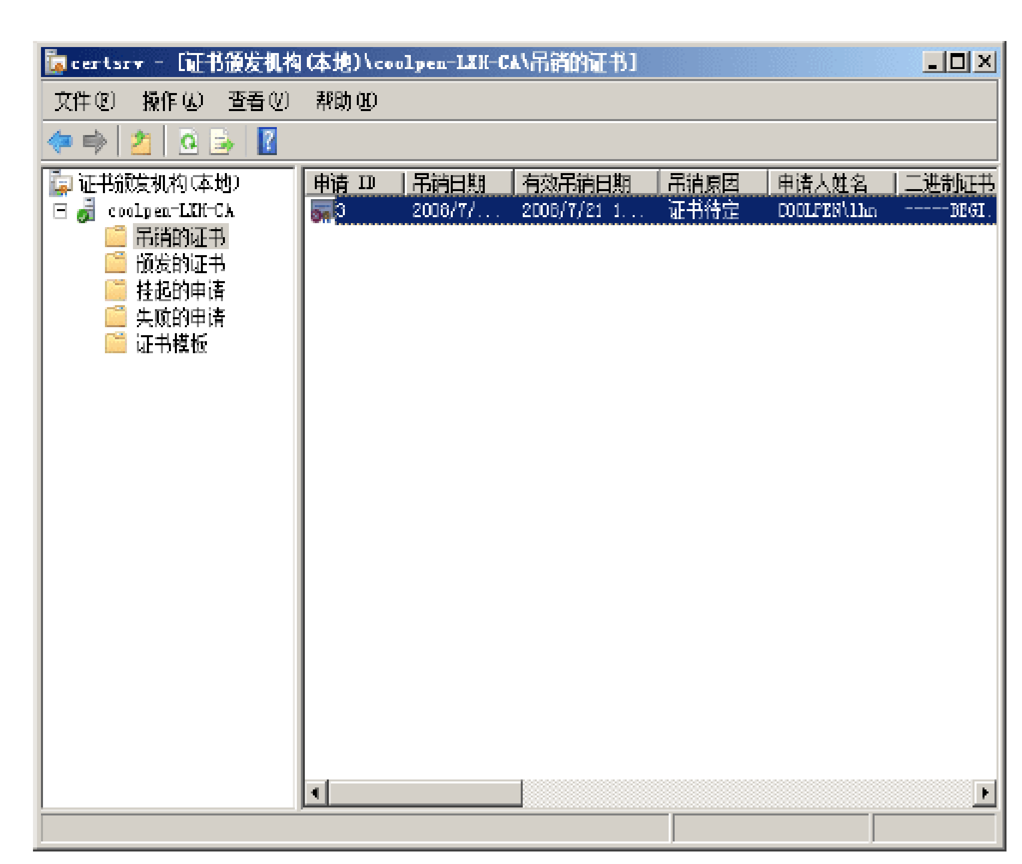


图 10.39 吊销的证书

10.6.2 解除吊销的证书

如果有些已吊销的证书需要继续使用，就可以将这些证书解除吊销。不过，需要注意的是，只有吊销原因为“证书待定”的证书才能解除吊销，其他原因吊销的证书将不能解除。

在“吊销的证书”窗口中选择欲解除吊销的证书，右击并依次选择快捷菜单中的“所有任务”→“解除吊销证书”即可。

如果证书不能被解除吊销，将显示如图 10.40 所示提示框，提示取消吊销失败。

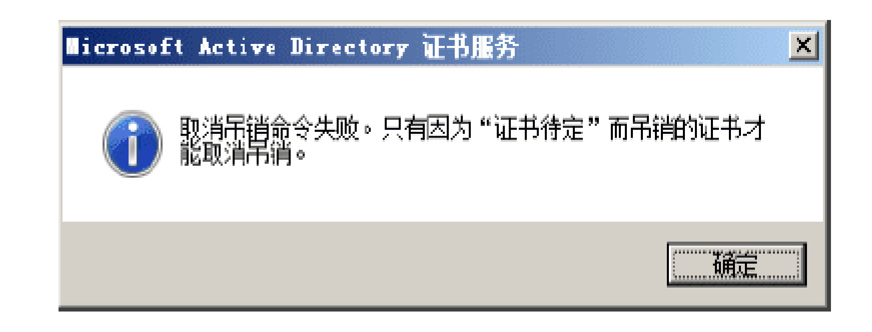


图 10.40 解除吊销失败

10.6.3 证书续订

证书都有一定的有效期限，当有效期过后，证书将会无效。因此，若要继续使用证书，就必须在证书到期前更新或者续订。证书的续订又分为用新密钥续订和使用相同密钥续订此证书。不过，只有登录到域以后才有权续订证书。

1. 用新密钥续订证书

01 在客户端计算机上运行 MMC 命令打开控制台，添加“证书”管理单元。依次展开“个人”→“证书”选项，选择欲续订的证书，右击并依次选择快捷菜单中的“所有任务”→“用新密钥续订证书”命令，



运行“证书注册”向导。单击“下一步”按钮，显示“申请证书”对话框，列出了可以请求的证书。单击“详细信息”按钮，可以查看该证书的详细信息。单击“注册”按钮，开始向证书服务器注册。完成后显示“证书安装结果”对话框，提示注册成功，如图 10.41 所示。

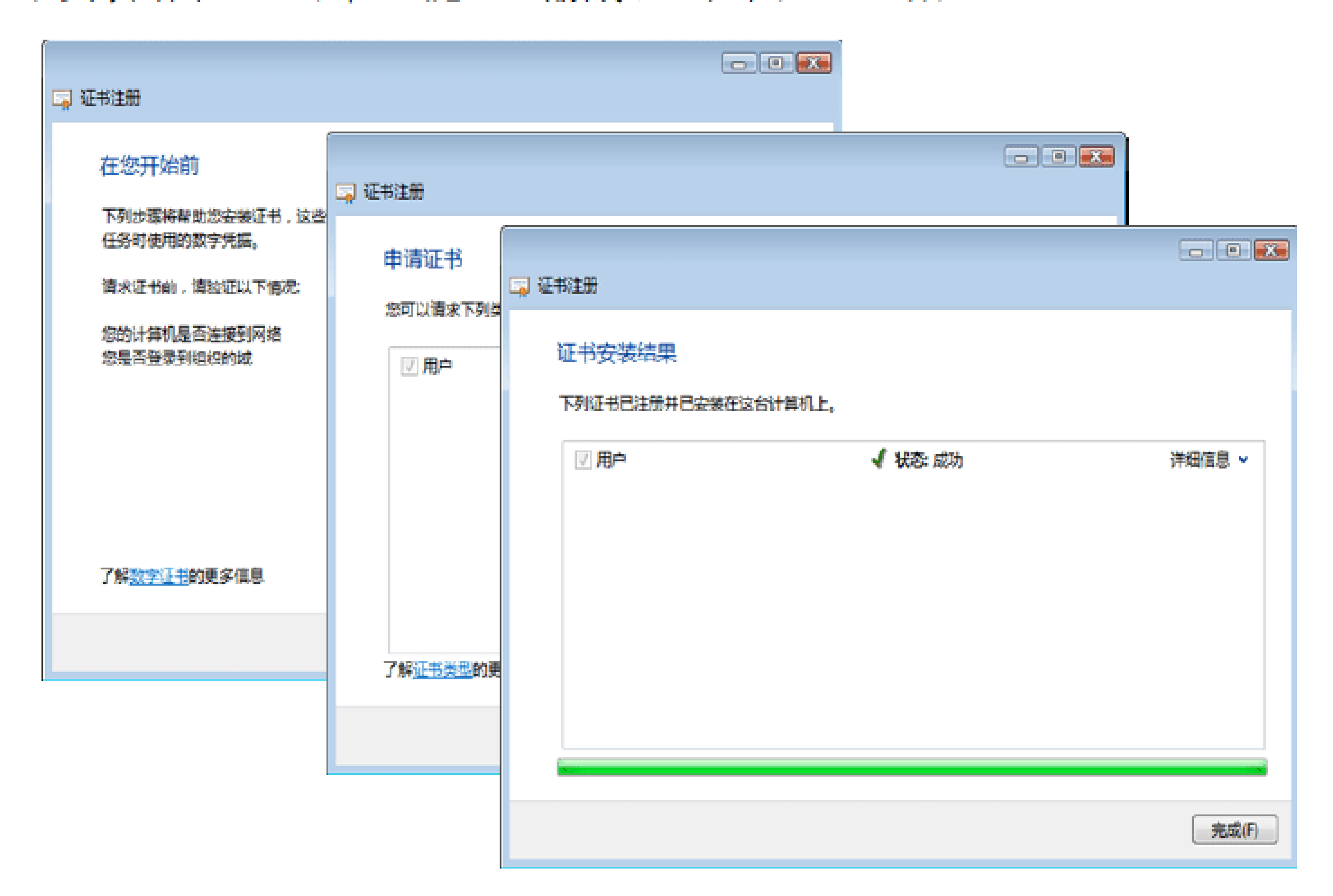


图 10.41　用新密钥续订证书

02 单击“完成”按钮，证书申请成功。

2. 用相同密钥续订证书

打开“证书”管理单元，选择欲续订的证书，右击并选择快捷菜单中的“所有任务”→“高级操作”→“使用相同密钥续订此证书”命令，运行证书注册向导。单击“下一步”按钮，显示“申请证书”对话框，列出了要请求的证书。单击“注册”按钮，开始向证书服务器注册，完成后显示“证书安装结果”对话框，单击“完成”按钮即可，如图 10.42 所示。



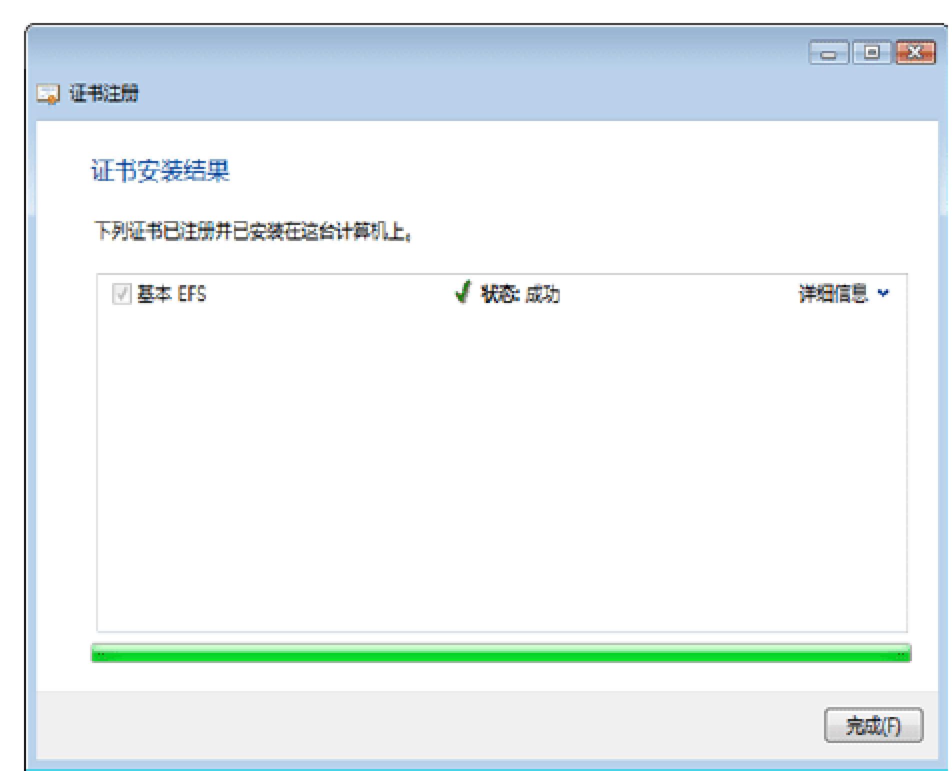


图 10.42　用相同密钥续订证书

10.7　证书服务安全现状

通常情况下，证书是为其他网络应用提供服务的，如电子邮件签名、安全站点搭建、电子

商务加密等。一旦证书泄露或被截获，将直接造成巨大损失。在活动目录中当部署证书服务的时候，可能会遇到以下各种问题：

- CA 密钥对丢失；
- 尝试修改证书模板；
- 尝试修改 CA 设置；
- 阻止证书吊销；
- 非授权的用户密钥还原；
- 独立管理员的 CA 问题；
- 附加不可信任的 CA 到信任根 CA 存储；
- 注册代理发布非授权证书。

10.7.1 CA 密钥对丢失

在 CA 密钥，可以对信息进行加密和解密。第一个密钥是私钥，第二个密钥是公钥。这两个密钥虽然不同，但在功能上是互补的。例如，公钥可以在目录证书中发行，方便组织中的其他人员可以对其访问。消息的发送方可以从活动目录中检索用户的证书，从中获取公钥，然后通过公钥对发送信息进行加密。接受方就可以通过私钥对其解密。

为了有效保护 CA 不受入侵者的攻击可以采用以下措施：

- 使用 FIPS140-2 来对 CA 密钥进行硬件保护。HSM 可以保护 CA 密钥使之处于安全令牌的保护之下，单独一个人是无法获取对密钥的访问权限的；
- 监测并控制本地管理员组成员，限制能够访问 CA 密钥的用户。

提示 

FIPS 是美国联邦信息处理标准的缩写，FIPS140-2 标准指定了密码模块需要被满足的安全需求，该模块被应用在安全系统之中保护敏感数据。HMS 是 Hierarchical Storage Management 的缩写，意为“分层存储管理”，可以自动地将访问频率较低的数据移动到较低的存储层次中，同时将访问频率较高的数据移动到较高的存储层次中。

10.7.2 修改证书模板

Microsoft 证书颁发机构支持 3 种类型的证书模板：版本 1、版本 2 和版本 3。在 Windows Server 2003 Standard Edition 和 Windows 2000 Server 设置的 CA 仅支持平版本 1 模板，在 Windows Server 2003 Enterprise Edition 和 Windows Server 2003 Datacenter Edition 设置的 CA 支持版本 1 模板和版本 2 模板，而 Windows Server 2008 上设置的 CA 支持所有这 3 个版本。版本 3 证书模板只能由客户端在运行 Windows Server 2008 或 Windows vista 的计算机上使用。

- 版本 1 证书模板。安装 CA 时会默认创建这些模板，但无法进行删除或修改，管理范围



十分有限；

- 版本 2 证书模板。允许自定义模板的大多数设置，如自定义是否能导出与证书相关的私钥、自定义证书模板支持的加密服务提供商（CSP）等；
- 版本 3 证书模板。允许管理员向其证书中添加高级 Suite B 加密设置。Suite B 加密设置包括数字签名、密钥交换和哈希的高级选项等。但版本 3 的证书模板只能在 Windows Server 2008 的服务器上安装且在 Windows Server 2008 和 Windows Vista 的客户端上使用的 CA 进行颁发。

如果入侵者获取了管理员级的权限，就能修改证书模板的属性，可以进行下列的恶意修改：

- 对于版本 2 证书模板，入侵者只能修改单个证书模板权限，但修改权限可以使入侵者能够注册一个具有额外权限的证书，从而能以其他用户的名义来请求额外的证书了；
- 对于版本 2 和版本 3 的证书模板，入侵者更改的范围将更加广泛，添加删除用户、证书模板替换等。

为了防范入侵者的入侵和恶意篡改，管理员应经常检查已部署的证书模板，确保与规划的相符合。未经验证的用户不能有对证书模板的读取和写入权限。

10.7.3　修改 CA 设置

如果入侵者得到了 CA 管理员权限，那么就可以修改 CA 设置。为了防范这种情况的发生，可以限制 CA 管理组中的成员，更改以注册表项的形式存储，设置成只有本地管理组的成员和具备 CA 管理权限的组才能对其进行修改。为了监测修改 CA 设置的用户可以开启针对 CA 的审核。

依次选择“开始”→“管理工具”→“Certification Authority”命令，显示“certsrv – [证书颁发机构（本地）]”窗口。右击“corp-WIN-HKSLEYF2MMT-CA”选项，在弹出的快捷菜单中选择“属性”选项，打开“corp-WIN-WIN-HKSLEYF2MMT-CA 属性”窗口，切换至如图 10.43 所示“审核”选项卡，选择需要审核事件的复选框，单击“确定”按钮即可。

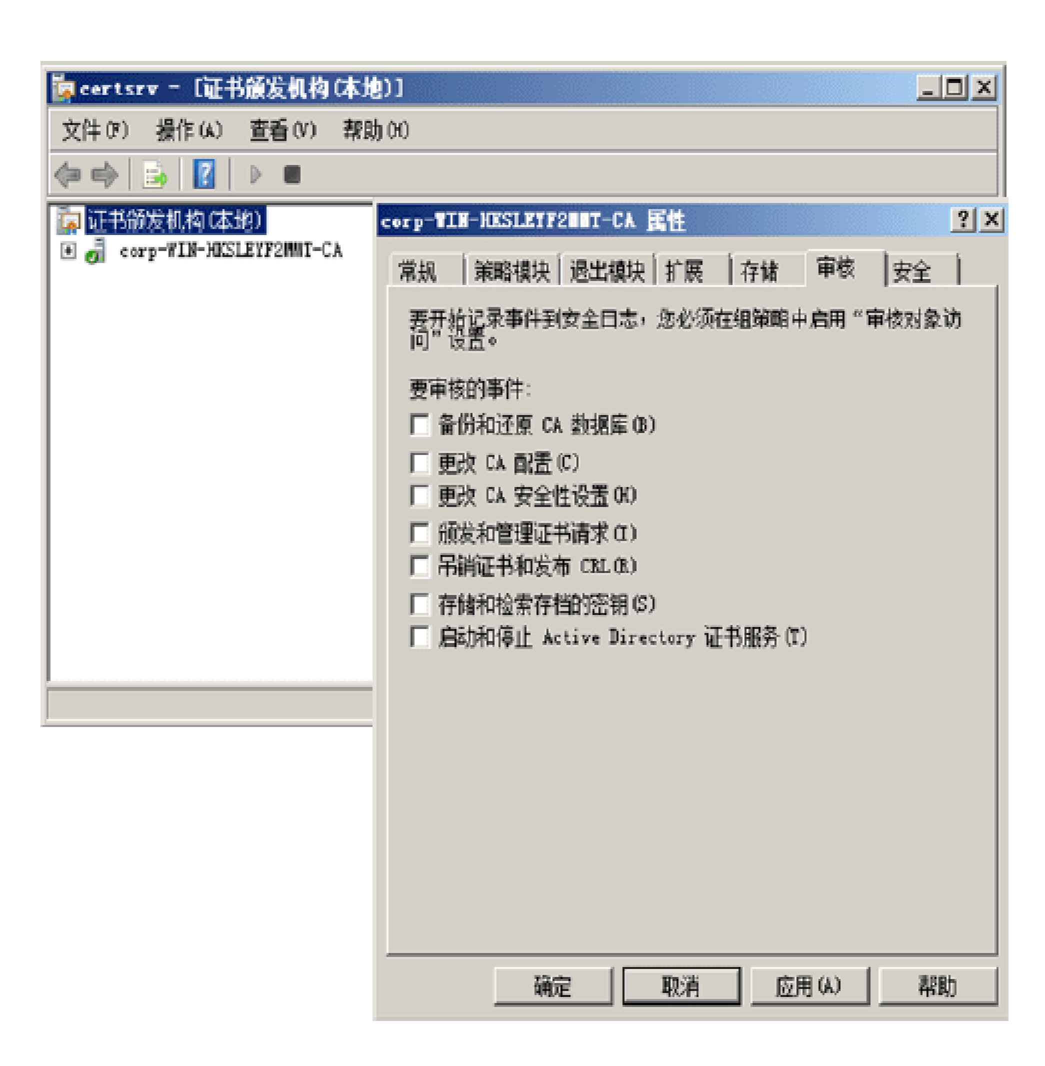


图 10.43　“审核”选项卡

10.7.4　阻止证书吊销

每一个证书都有一个使用期限。吊销证书就是证书在还没有到有效期前不能作为有效的受信任的安全凭据。入侵者常常使用各种方法阻止证书的吊销，从而进行非法活动，通常使用以下方法：

（1）入侵者可以阻止软件证书的吊销检查

例如，在 Internet Explorer 7.0 中，默认会自动检查证书的吊销状态，如图 10.44 所示“Internet 选项”对话框。

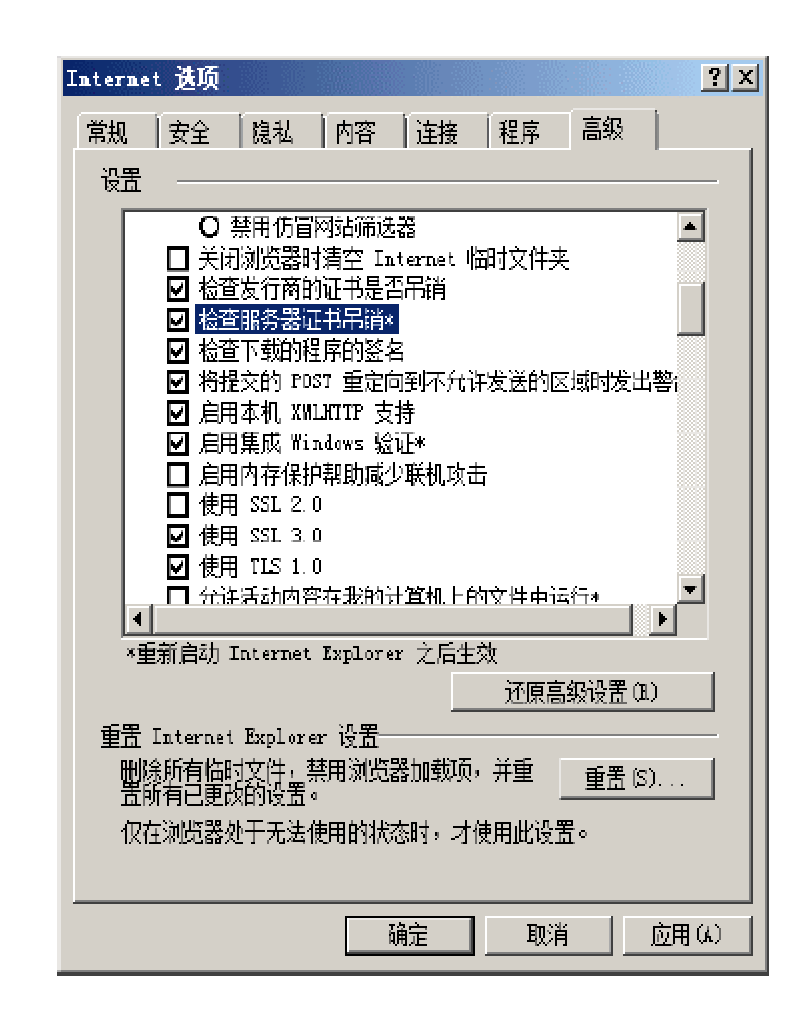


图 10.44 “Internet 选项”对话框

（2）入侵者可以阻止访问 CA 或是 CRL 证书服务器

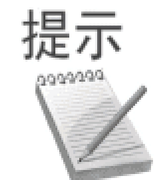
如果某程序没有缓存正确的 CRL 或是 CA 证书版本，那么该程序将会尝试以下列方式获取：

- 如果某证书已更新，则可以从 AIA（授权检验机构）下载证书。
- 可以从 CRL 下载基础 CRL 或是 DELTA CRL。

（3）入侵者可以阻止对作为 OCSP（在线证书状态响应协议）响应的服务器群的访问

一个 OCSP 客户端发布一个状态查询给一个 OCSP 响应器并且监听当前证书直到响应器提供一个响应。OCSP 协议表述了在应用程序检查证书状态和服务器提供状态之间所需要交换的数据。证书状态值中使用了一些确定回复识别：

- 良好。表示一个对状态查询的积极回复，这个积极回复表示这张证书没有被撤销，但不一定意味着这张证书曾经被颁发过或是产生这个回复在证书有效期内。
- 已撤销。表示证书已经被撤销，无论是临时性的还是永久性的。
- 未知。表示响应器不知道请求的证书，如果 OCSP 客户端无法与 OCSP 响应器通信，则程序就会吊销证书。

提示  如果使用 OSCP 来进行对证书的吊销检查，则必须确保 OCSP 响应器对于所有证书的吊销检查都是可用的。

10.7.5 授权的用户密钥还原

在 Windows Server 2008 Enterprise 或是 Windows Server 2008 Database 中，允许用户通过加密证书对密钥进行各种操作。

如果入侵者既有证书管理员权限又有密钥恢复权限，那么他就可以从 CA 数据库中截获用户的证书和密钥，能够解密被证书所保护的信息。即使用户启用了签名，入侵者也能够模仿用户的数字签名。

10.7.6 附加不可信任的 CA 到信任的根 CA 存储

如果入侵者将不可信任的 CA 添加到信任根 CA 存储，则该证书将连到信任根 CA 证书中



的全部证书，都会被认为是可信任的。

在 Windows Server 2008 中，默认的防范伪根 CA 证书的机制有以下几种：

- 用户帐户控制。只有本地管理员组的成员才可以添加根 CA 证书到计算机的信任根存储中。如果入侵者做了一个伪根证书，则 UAC（用户帐户控制）就会向客户端发出警告；
- 信任根组策略。组策略允许用户定义添加的根 CA 证书规则；
- 管理域的受信任根证书。

01 依次选择“开始”→“管理工具”→“组策略管理”选项，显示如图 10.45 所示的“组策略管理”窗口。

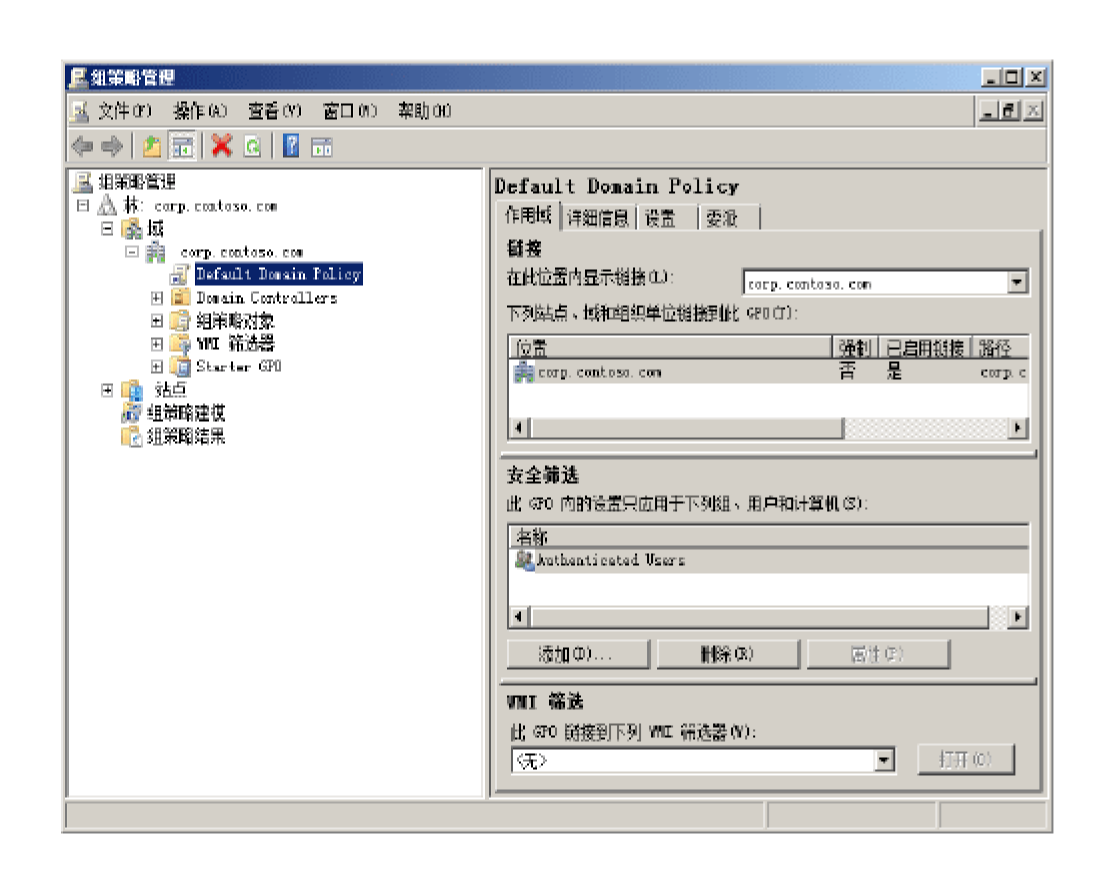


图 10.45　“组策略管理”窗口

02 选择“林：corp.contoso.com”→“域”→“组策略对象”，右击“Default Domain Policy”选项，在快捷菜单中选择“编辑”选项，显示“组策略管理编辑器”窗口。依次选择“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“公钥策略”选项，在右侧窗格中双击“证书路径验证设置”选项，显示如图 10.46 所示“证书路径验证设置 属性”对话框。

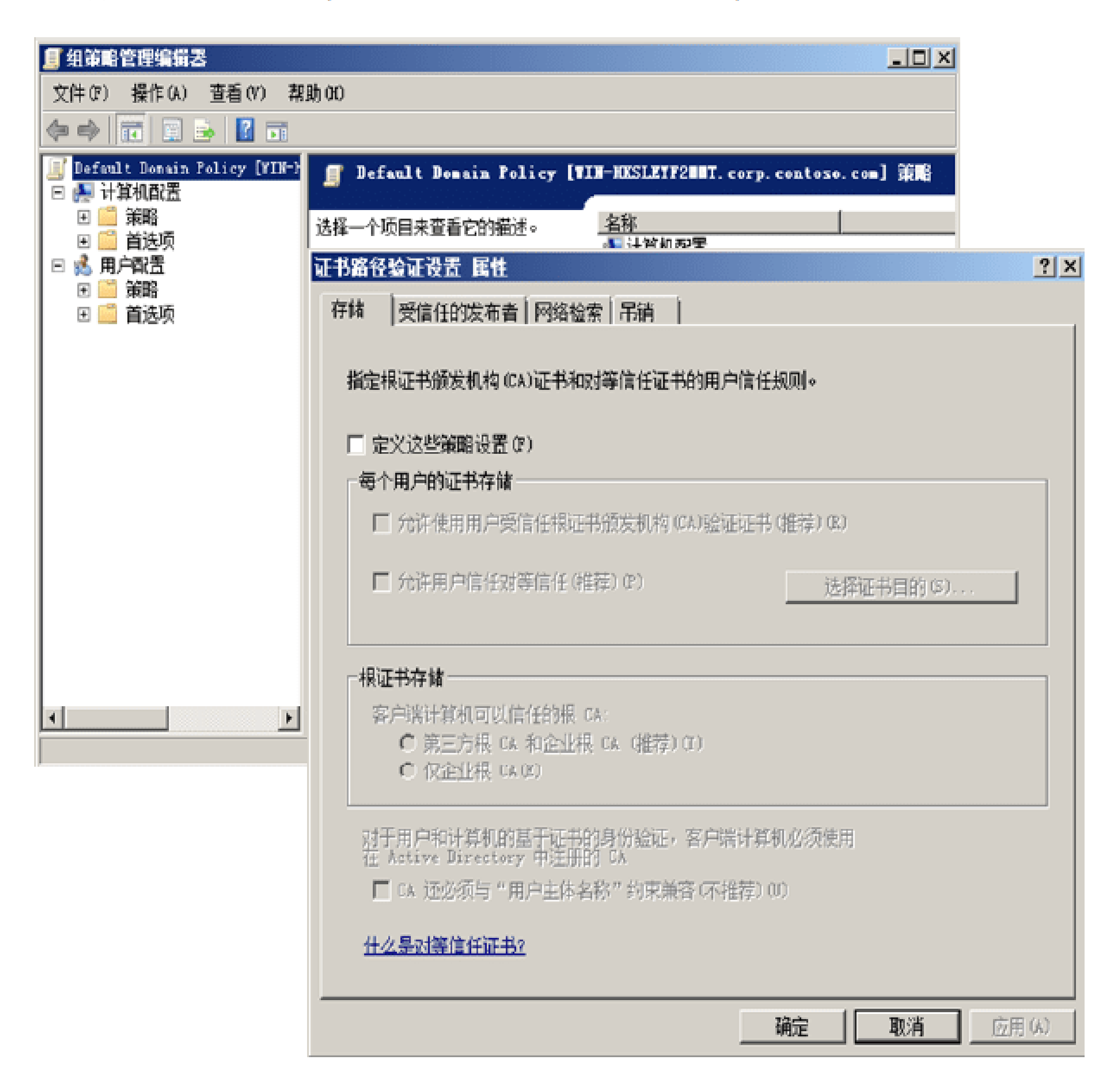


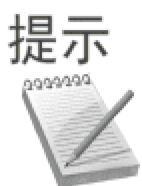
图 10.46　打开“证书路径验证设置 属性”对话框

03 选择“存储”选项卡，选中“定义这些策略设置”复选框，根据需要选择相关设置，单击“确定”按钮即可。

10.7.7 注册代理发布非授权证书

在 Windows Server 2008 中，允许用户强制限制注册代理，通过该功能可以限制指定为注册代理的用户所拥有的代表其他用户注册智能卡证书的权限。可以通过以下两种方法限制注册代理：

- 基于证书模板预定义列表的证书来限制注册代理；
- 进一步限制使用智能卡注册的组。

提示  受限注册代理是 Windows Server 2008 企业版系统中的新增功能，在基于 Windows Server 2008 标准版的 CA 上，受限注册代理不可用。

10.7.8 独立管理员的 CA 问题

在 Windows Server 2008 中，默认赋予内置管理员组执行所有的管理任务的权限。如果使用证书服务的计算机是一个独立计算机，那么管理权限将分配给本地管理组。如果计算机是域成员，那么管理权限分配给企业管理员和林中创建的第一个域的管理组。

这样的默认权限赋予会使得管理员组中的所有成员都可以执行任意的管操作。这会让恶意管理员能够修改 CA 设置，吊销证书和删除审核日志。为了减小此威胁 Windows Server 2008 提供了四种 PKI 管理角色：

- CA 管理员，负责帐户管理和 CA 证书的密钥生成；
- 证书管理员，负责证书的管理，包括发布和吊销证书及解压密钥等；
- 审核员，负责维护和设置 CA 审核日志；
- 备份操作员，负责 PKI 信息的备份。

在 Windows Server 2008 企业版和 Windows Server 2008 数据中心版中允许用户强制 Common Criteria 角色的隔离，一个用户只能是 CA 管理员、证书管理员、审核员和备份操作员中的一个角色。如果一个用户具有两个或两个以上的角色，该用户就会被锁定，将无法进行证书管理操作。

提示  本地管理员可以在命令提示符窗口中，使用“certutil-setreg ca\RoleSeparation Enabled1”来启用 Common Criteria 强制角色隔离。

小　　结

证书在网络中应用非常广泛，安全 Web 连接的站点（使用 HTTPS）、邮件的签名和加密、网上银行在线交易等都需要证书来保护信息的安全。通过部署 Windows Server 2008 自带的证



书服务功能，可以实现不同类型数字证书的颁发，即可实现安全连接、数据加密等功能。Windows Server 2008 支持两种证书服务器，分别是应用于企业内部的企业证书服务器和应用于企业或 Internet 的独立证书服务器。企业 CA 的安装建立在 AD DS 的基础上，而独立根 CA 则是建立在独立服务器的基础之上，与 AD DS 无关。

习　　题

1. 什么是电子证书服务？
2. 企业证书和独立根证书有什么区别？
3. 实现证书续订有哪几种方式？
4. 解除吊销证书的前提是什么？

实验：配置和应用证书服务器

实验目的

掌握证书服务器的基本应用。

实验内容

安装企业证书服务器，并用两种方式向服务器申请证书。同时，备份证书服务器中的证书。掌握客户端证书续订的方法。

实验步骤

1. 安装企业根证书服务。
2. 使用“证书申请向导”申请证书。
3. 使用 Web 方式申请企业证书。
4. 备份证书服务器上的证书。
5. 用相同密码续订证书。

Windows Server 2008

第11章

系统服务安全

Windows Server 2008 本身就是多业务服务器操作系统，默认已经集成了多种常用网络服务和系统服务，管理员根据需要安装或者启用即可。但是，从系统安全角度考虑，每一种应用都可能存在安全漏洞，运行的服务越多，系统安全性就越低。因此，对常用系统服务功能及特点加以了解，并且能够通过各种安全机制确保服务 Windows 系统服务的安全，是非常有必要的。

本章导读

- 服务概述
- 针对服务的攻击
- 普通服务攻击媒介
- 服务强化
- 服务安全

11.1　服务概述

服务为用户帐户、应用程序以及 Windows 本身，提供客户端和服务器之间的连接机制。有些服务是 Windows 执行功能所必须的，而其他服务只是在执行特定任务时才需要。服务在会话 0 中启动，其中包括系统完整性、数据执行保护（Data Execution Prevention，DEP）和服务安全标识符（Service Security Identifier，SID）。与普通应用程序不同的是，服务有特殊的 SID，可进行细粒度访问控制。

11.1.1　服务登录帐户

每个服务都被指派了一个服务登录帐户，该帐户决定了服务运行的安全上下文。内置服务登录帐户包括本地系统，本地服务和网络服务；而管理员和开发者可随意创建或定义新的帐户。服务登录帐户的权限是决定某一特殊服务能够访问本地或网络资源的主要方法。

1. 内置服务登录帐户

如表 11.1 所示列出了内置服务登录帐户以及与本地和远程资源的相互作用。

表 11.1　内置服务登录帐户

登录帐户名	本地资源	网络资源
Local System（经常指的是 Localsystem 或是 System，以 NT AUTHORITY\标签来表示）	计算机上最高特权的帐户，可以实现对所有资源的完全访问	连接到帐户所在计算机的网络资源
Local Service（经常以 NT AUTHORITY\标签来表示）	具有一般的访问权限，分配给已经过验证的用户，其有稍多的特权	作为空（匿名资格）会话帐户连接到网络资源
Network Service（经常用 NT AUTHORITY\标签来表示）	与 Local Service 一样，其具有一般的访问权限，分配给已经过验证的用户，具有多一些的特权	与 Local System 帐户一样，作为计算机连接到网络资源。远程令牌包括每个人和已经过验证用户 SID

服务可以使用内置服务登录帐户，也可使用任何有效的本地或域用户帐户。在早期 Windows 版本中，所有 Windows 提供的服务都在本地系统上下文中运行。但是，这个策略不符合最小特权原则。从 Windows XP 开始，Microsoft 创建了更具局限性的本地服务和网络服务帐户，另外，开发和配置服务遵循最小特权原则。

服务登录帐户用于本地和远程资源的验证服务，使用 Kerberos 验证（代替 NTLM 或 LM）的服务也需要分配给服务登录帐户一个或多个服务主要名称（Service Principal Names，SPN）。SPN 用于识别服务，在客户端应用程序和服务之间进行相互认证。

2. 服务控制管理器

所有服务登录帐户都必须分配一个登录的服务权限，这样才可以通过服务控制管理器（Service Control Manager，SCM）控制该服务，并且在无需外部安全主体登录的情况下，能够登录和访问资源。

SCM 作为远程过程调用（Remote Procedure Call，RPC）服务器，在 Windows 启动过程中启动，因此服务管理和控制程序（Sc.exe、Services.msc、WMIC，等等）可以与本地和远程服务相互通信。SCM 会读取位于注册表中的服务值，使用已找到的凭据在本地计算机上登录服务帐户，加载服务帐户文件，并以暂停状态开始服务。然后，将服务与服务帐户登录令牌关联，从而完成服务的启动过程。SCM 会检查所有注册的服务依据，并在需要时将其启动。

SCM 有很多基于服务的任务，包括：

- 维护安装服务的数据库；
- 在系统启动时或用户要求时启动服务；
- 列举已安装的服务和驱动服务；
- 维护运行服务和驱动服务状态信息；
- 传递控制请求以运行服务；
- 锁定和解锁服务数据库。

当需要启动服务时，SCM 为服务登录帐户创建一个登录会话，加载相关的登录帐户用户信息，然后启动服务。如果 SCM 正常工作，其会将进程令牌（带有服务 SID 和特权的令牌）附加到服务进程上。

每种服务的配置信息都存储在 HKLM\System\CurrentControlSet\Services 的 Windows 注册表中。如图 11.1 所示是 Dfs 服务的注册表项。

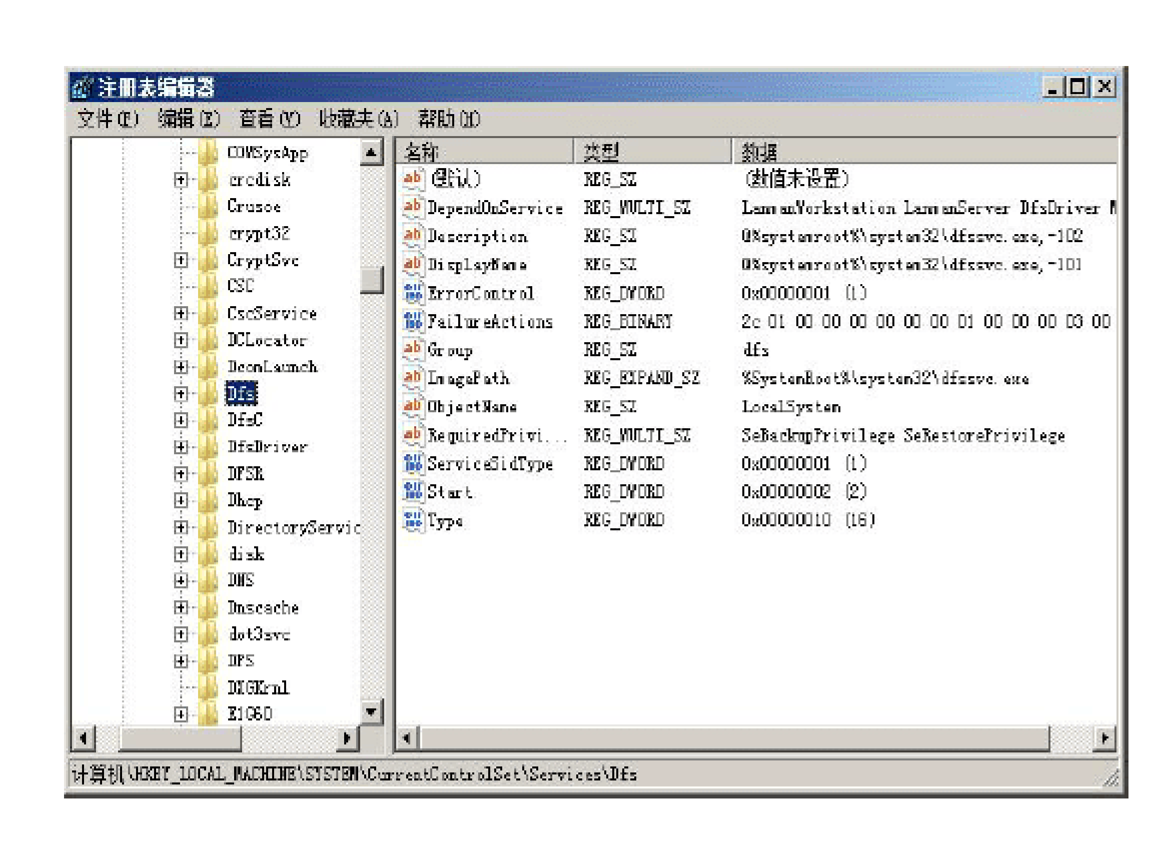


图 11.1　服务的注册表项

服务和驱动都位于服务注册表项中，可以通过 Type 键值来辨别服务。例如，0x10（作为独立程序，运行于自身进程中的服务）或 0x20（运行于共享进程中的服务）。驱动的 Type 键值为 0x1（核心驱动）或 0x2（文件系统驱动）。除此之外，服务的 Start 键值通常为 2（自动）、3（手动）或 4（禁用），而驱动的初始值为 0（启动）或 1（系统）。

所有的服务登录帐户都有其相关的密码。Windows 分配给内置服务帐户的密码又长又复杂。管理员不能轻易列举密码，也无需更改密码。通常服务登录帐户密码由管理员设置，存储在受保护的本地注册表，本地管理员能够通过特殊的软件列举出所有服务帐户密码。

11.1.2　服务监听端口

多数服务都有一个端点监听句柄来接收和发送服务的相关信息。通常情况下该句柄使用

TCP 或 UDP 端口号（如终端服务在 TCP 端口号为 3389）和 IP 地址来表示，服务也可使用 RPC、命名管道或另一种有效的监听协议（例如 net.msmq）进行监听。服务的监听 TCP/IP 端口可使用 Windows 进程管理器或在命令行中使用 netstat –anob 列举。

如果服务使用 TCP 端口号，通常情况下，将会默认使用 TCPv4 和 TCPv6 进行监听，如图 11.2 所示。如果监听端口的 IP 地址为 0.0.0.0，则该服务将响应所有连接端口，包括本地主机。如果监听端口的 IP 地址为 127.0.0.1，则该服务只响应与本地主机的连接尝试。如果服务在一个特殊的 IP 地址（例如 192.168.1.10）上监听，服务将只响应与该 IP 地址的连接尝试。

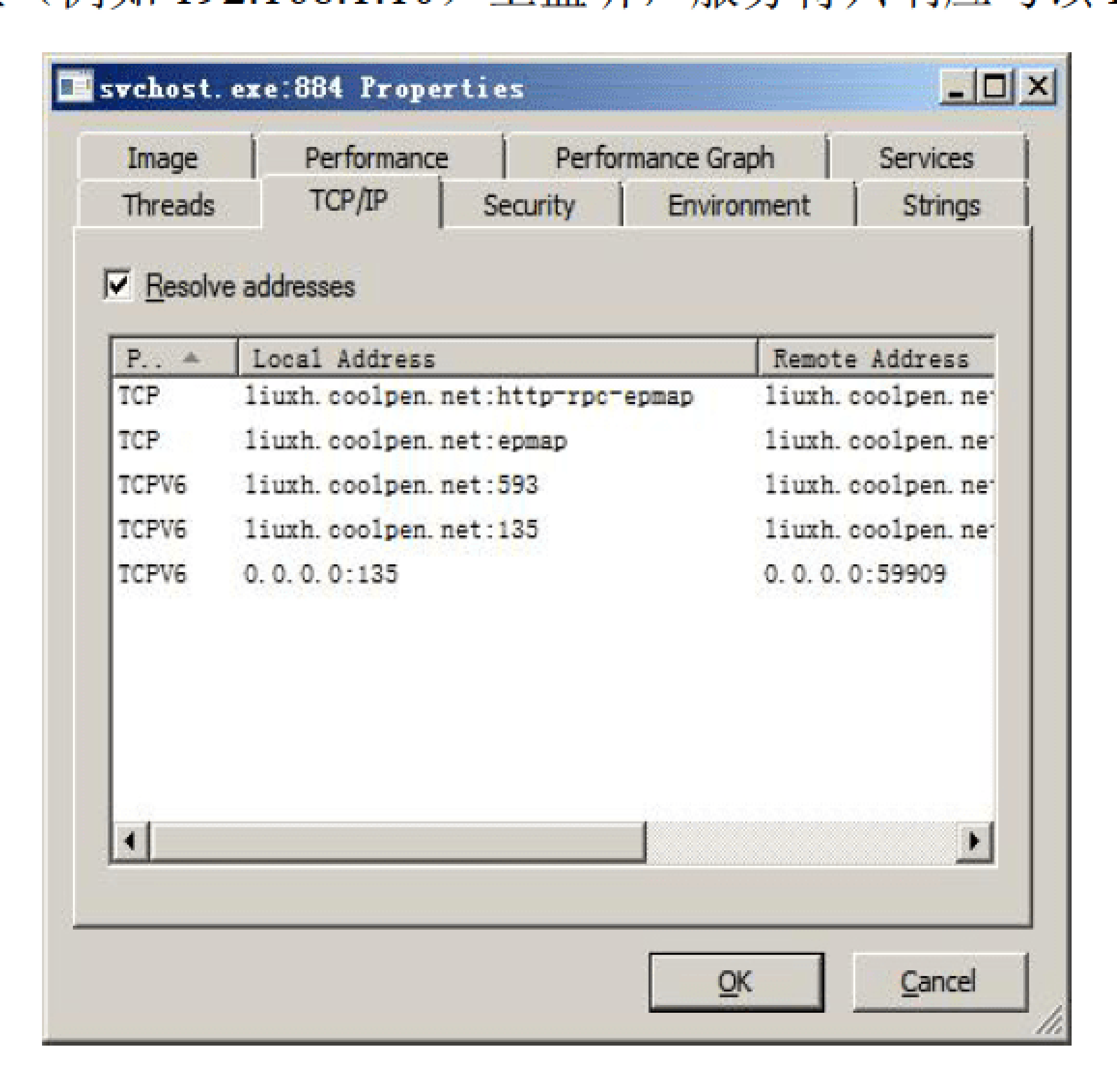


图 11.2　使用进程管理器的 TCP/IP 标签来表示监听端口号

11.1.3　配置服务

服务在运行时，不一定有图形用户界面，但所有服务的信息，都可以通过软件或服务控制台（Services.msc）进行配置和管理，这些信息存储于注册表中供 SCM 读取。用户可以双击任何服务名称查看其详细内容。普通用户可以看到服务信息，但只有帐户操作员（Account Operators）、域管理员（Domain Admins）或企业管理员组（Enterprise Admins groups）的成员能够进行修改。

1. “常规”选项卡

“常规”选项卡是打开服务属性对话框时默认显示的选项卡，如图 11.3 所示。“服务名称”是 Windows 中的内部名，即服务的短名称，服务管理工具通常使用服务名来操作特定的服务。在“服务”控制台中，“显示名称”是服务在列表中最显著的标签。“说明”则是开发者创建的关于该服务的简短描述和说明信息。



图 11.3　查看和配置系统服务

可执行路径显示了可执行服务的全部路径，有时恶意软件会使用和 Microsoft 服务名相似的名字，在解决这类问题时，可执行领域路径很有帮助。例如，恶意软件名为 svchost.exe，但却位于\Windows\Fonts 文件夹，而不是在通常的\Windows\System32 文件夹中。

启动模式很重要，可以将其配置为以下 4 个值之一：

- 自动（延迟启动）;
- 自动;
- 手动;
- 禁用。

“自动”（延迟启动）是指 SCM 在所有其他服务都设为自动值（包括其依赖的服务）时启动服务。该选项是在 Windows Vista 引入的。根据注册表项所定义的顺序，服务设置为 Windows 启动过程中自动启动。如果标注为“自动”的服务取决于其他服务是否启动，则必须先启动这些服务（除非是标记为“禁用”）。设置为“手动”的服务，则不会在 Windows 启动过程中自动启动，除非其他服务或应用程序要求其启动。许多设置为“手动”的服务在需要时才启动，不需要时就停止。SCM 不能启动设置为“禁止”的服务，如果不改变其所定义的值，也不能手动启动。

“状态”显示服务目前的操作状态。操作状态有“已启动”、“已停止”和“暂停”等 3 种。“暂停”并不是像大多数用户想象的那样，其并没有停止服务。服务仍在内存中活动，并且可以完成当前请求，但不能执行更多要求。服务与 SCM 相互作用，并在需要时采取适当的行动。基于安全性和可靠性，许多默认的 Windows 服务不能暂停。启动参数允许服务在运行过程中执行更多的参数、指令和命令。

2. “登录”选项卡

“登录”选项卡（如图 11.4 所示）决定与服务有关的服务帐户，以及桌面交互和硬件需求。

在登录框中，用户可以设置在本地系统上下文中运行的服务或输入服务名，包括本地服务、网络服务以及其他有效服务名。登录帐户存在于本地 SAM 数据库或活动目录中。如果服务帐户没有以服务身份登录的权限，在设置过程中应授予其相应的权限。即使是不需要输入密码的本地系统、本地服务或网络服务，在这里也必须输入服务帐户的有效密码。密码会存储于注册表中，便于 SCM 以后使用。

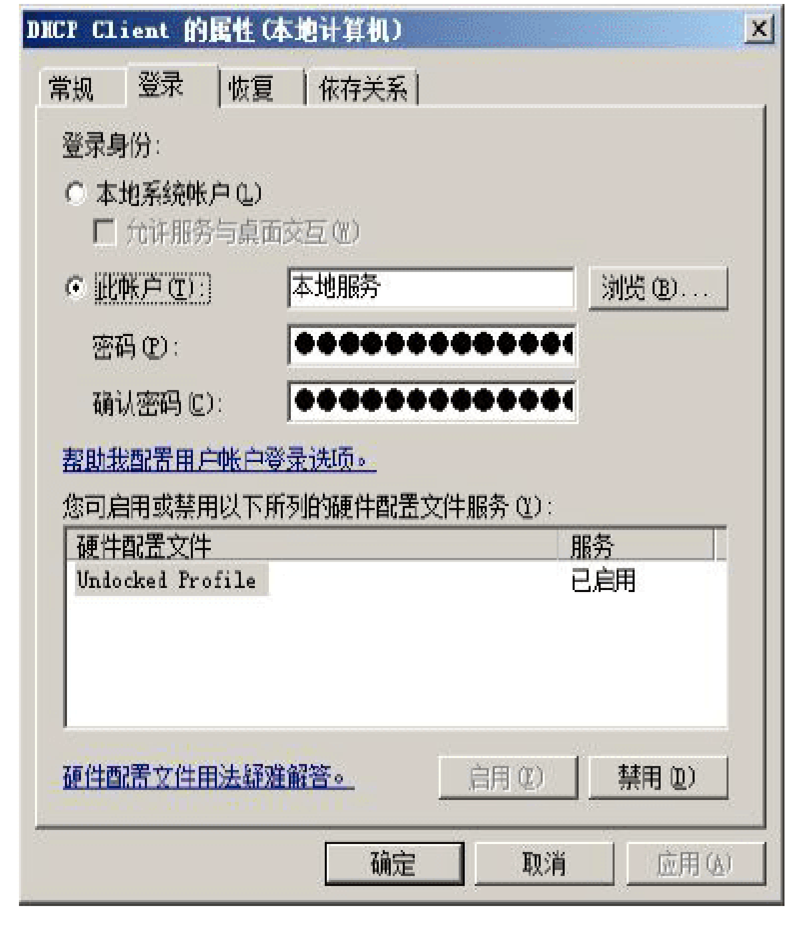


图 11.4 “登录”选项卡



注意 在此不能检验在登录选项卡中所输入的密码是否正确。只要相同的密码输入两次，即使密码不正确，SCM 也会接受此密码并将其存储，当然，服务是无法启动的。

选中“允许服务与桌面交互”复选框时，将允许服务与桌面间进行交互。事实上，某些服务需要该选项才能与用户进行沟通。后台打印服务和交互式服务检测服务都需要桌面交互。在多数情况下此选项是不允许的；一旦允许，会对终端用户、桌面、服务和其他计算机造成安全

威胁。例如，如果允许服务与用户桌面交互，终端用户或运行于终端用户安全上下文的恶意软件就可以很容易的操纵该服务。服务也很容易影响同一计算机上的其他用户和桌面。限制服务与用户桌面之间的交互是未来的发展趋势，从这一点来看，很多旧的服务都是不合格的。

用户也可以在“硬件配置文件”中允许或禁止某项服务。此选项通常用于拥有扩展坞的笔记本电脑。在特殊的硬件配置文件中，若不需要某项服务，就要将其禁止，以防范恶意入侵者的攻击。当然，这样做也可以提高系统性能和节约能源，笔者觉得这才是微软的主要目的。

3. “恢复”选项卡

“恢复”选项卡（如图 11.5 所示）定义了当某一服务失败时，应当采取何种反应。可以选择以下几种方法：

- 不操作；
- 重新启动服务；
- 运行一个程序；
- 重新启动计算机。

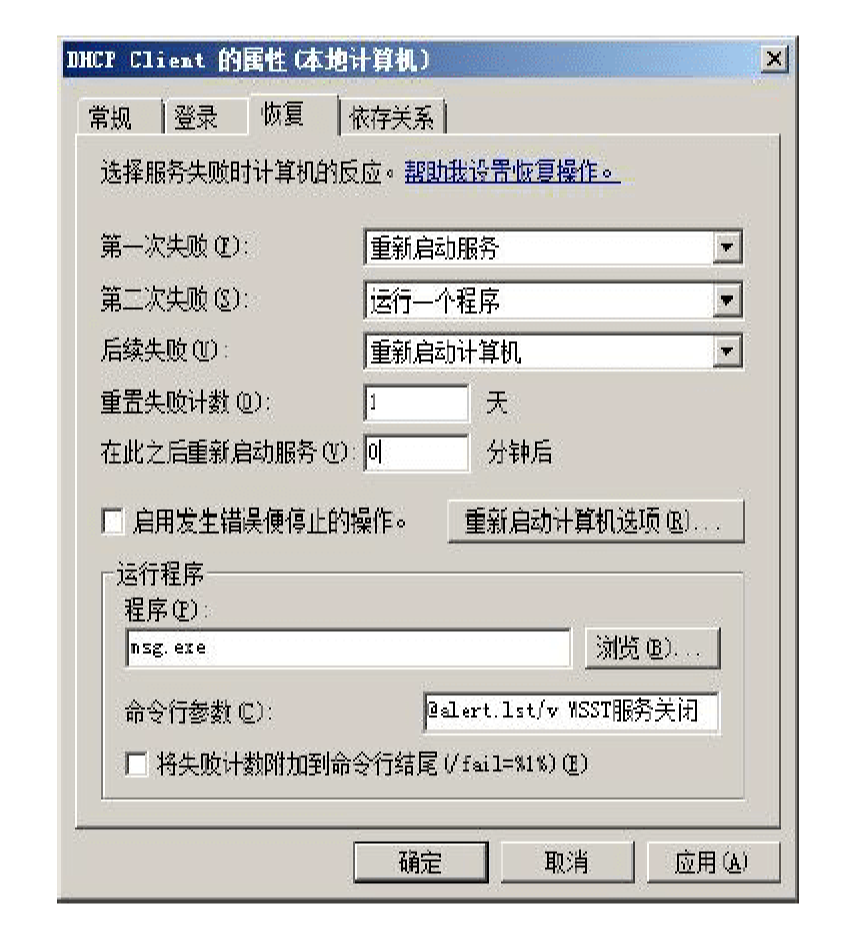


图 11.5　“恢复”选项卡

既可以定义“第一次失败”、“第二次失败”和“后续失败”的反应，也可以设定在一段日期之内失败计数器被重置了多少次。例如，如果“重置失败计数”设置为 1 天（通常值），24 小时后计数器会重新设置为 0，遇到服务失败就会执行第一次失败的反应。如果错误计数器设置为 0，说明如果不重启计算机，计数器就不会重置。如果还原行为设置为重启服务，可以在重启服务前指示 SCM 要等多久再重启。

如果选择“运行一个程序”恢复选项，该程序或其他脚本可以在服务失败后运行。图 11.6 为使用 Msg.exe 程序向预定清单上的用户发送“WSST 服务关闭”信息。使用此功能，会弹出帮助窗口来调查失败服务或运行一个新的调试程序。另外一个作用是在重启服务后，使用网络监测功能截获该服务发送和接收的网络数据包，为故障调试提供帮助信息。截获的信息对识别恶意连接十分有用。需要使用驱动器名称和完整路径来定位可执行文件，不支持 UNC 形式的路径（例如\\服务器\共享名）。



注意　在 Windows XP Professional SP2 之前，管理员可以使用 NET SEND 来发送信息。但由于 NET SEND 是基于不安全的 Messenger 服务的，因此在 Windows Vista 和 Windows Server 2008 中使用 Msg.exe 代替 NET SEND。

微软考虑到由于服务重启或失败会导致计算机重启，所以在重启前向用户发送信息以示警告。单击“重新启动计算机选项”按钮，显示如图 11.6 所示“重新启动计算机选项”对话框。

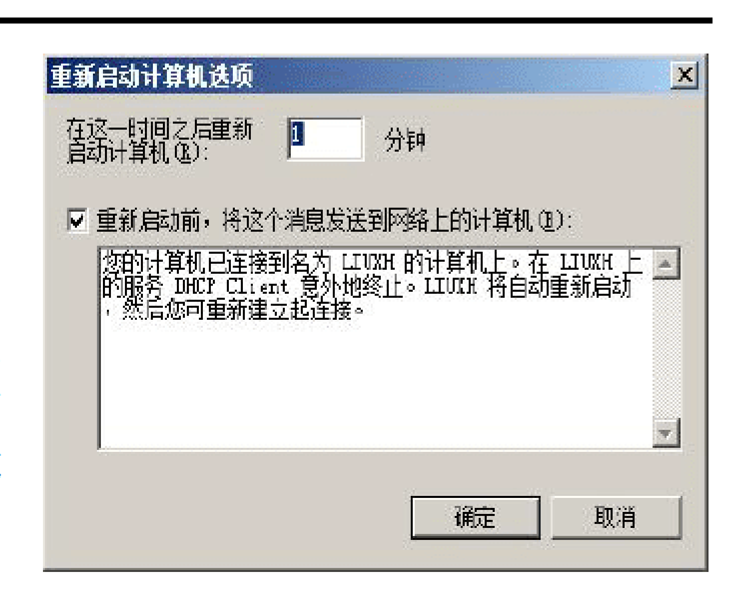


图 11.6　重新启动计算机选项

不过，自动“重新启动服务”的还原选项会给入侵者提供攻击计算机的机会。例如，地址空间布局随机化（Address Space Layout Randomization，ASLR）在每次启动计算机时，随机将核心 Windows API 置于 256 个不同的存储地址。许多缓冲溢出区要求只有猜到正

确的 API 地址时才能得逞，否则攻击就会失败。如果某服务在失败后自动重启，这就给入侵者提供了一个很好的机会，使其在经过数次尝试后得知正确的存储地址。

4. “依存关系”选项卡

“依存关系”选项卡（如图 11.7 所示），显示了某服务运行所依存的所有服务。在服务控制台中还有很多不能看到或进行设置的服务值（在本章后面将会讲到），其中包括许可、权限以及服务是否可以停止或暂停。除了服务控制台之外，还可以用其他方法来设置服务，包括组策略、sc.exe 和 Windows 管理规范（Windows Management Instrumentation，WMI）以及其他一些方法。

服务失败可能是操作或者安全因素导致的，尽管其通常不是恶意行为，但很多恶意软件（MS-Blaster 蠕虫、DDoS 等）也会导致某些无法解释的服务问题。

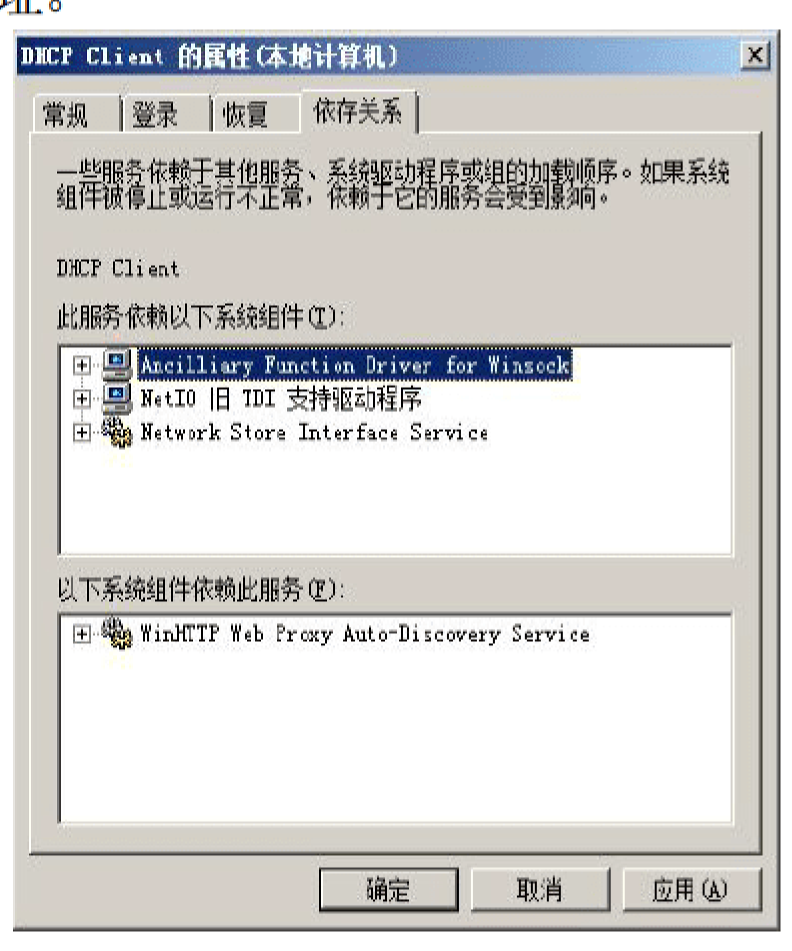


图 11.7 “依存关系”选项卡

11.2 针对服务的攻击

如今，网络入侵方式可谓花样繁多，其实很多服务是针对系统服务或网络服务的。由于 Windows 系统默认自动启动了许多服务，而每一种服务就像是一扇开启的大门，在允许用户正常使用的同时，随时可能成为入侵者的进攻渠道。为此，管理员应对常见的基于系统服务的攻击和入侵有所了解，以便及时做好防护工作。

11.2.1 Blaster 蠕虫

Blaster 蠕虫是 2003 年最为臭名昭著的蠕虫病毒。在运行 Windows 2000 和 Windows XP 的计算机上，Blaster 攻击 Windows DCOM RPC 服务中已知的缓冲区溢出漏洞。虽然漏洞已知，也可以进行 Microsoft 安全更新，然而大部分的计算机并没有更新。大部分用户错误地认为，正确设置的外围防火墙能够有效地防止 Blaster 进入网络。

Blaster 与 TCP 端口 135 的 DCOM RPC 服务连接，对缓冲溢出区进行攻击。一旦系统出现漏洞，Blaster 就可以对系统进行本地访问，并在 TCP 端口 4444 启动一个新的界面，使用 UDP 端口 67 上的 TFTP 下载其余的病毒。该病毒会将自身重建在名为 msblaster.exe 的文件中，这是一个自动运行的注册表位置。之后病毒会重启计算机，开始用该主机去感染其他计算机。

Blaster 刚开始出现时，很多组织并没有重视该病毒，由于人们认为在本地计算机上正确设置的外围防火墙（不允许 TCP 端口 135 的入站访问）能够有效的抵制 Blaster 感染。但是，受感染的计算机通过 VPN 连接到网络，导致凡是没有安全更新的计算机都被感染了。只要由一台感染病毒的计算机，网络中其他易受攻击的计算机都难以幸免。Blaster 可以在短时间内

感染成千上万的计算机。

Nachi 是一种与 Blaster 非常相似的蠕虫病毒。该病毒是在计算机进行错误更新之后数天内出现的，以 Blaster 同样的方式感染易受攻击的计算机，感染后将自动使计算机安装安全更新，防止计算机被 Blaster 感染。这是一个典型的示例，说明不提示用户而自行修补计算机的恶意软件是多么的危险。Nachi 指示网络中所有易受攻击的计算机同时下载安全更新，占据了庞大的网络资源。当安装了更新之后，Nachi 就置身事外，不再对计算机进行保护。Nachi 会带来漫长的下载时间和更多的安全问题，因此，也就比 Blaster 更加危险。

为了防止 Blaster 攻击，微软对其操作系统做了很大的改变，尤其是在计算机自动安全更新方面。鉴于 Windows 用户一直以来都使用 Windows Update 和其他更新客户端，微软推出了新的自动更新服务，包括升级版的自动更新，并为没有使用其他补丁管理策略的企业提供免费的软件更新服务和 Windows 服务器更新服务。系统安装操作更加简单易行，并且在安装更新前，网络访问是受限的，从而确保计算机的攻击面最小化。

11.2.2　普通服务攻击媒介

每个安装和运行的服务都是入侵者的一个攻击媒介，对于常规系统应用而言，常见的攻击威胁如下。

1. 缓冲区溢出

所有服务都提供远程访问的监听通道，当服务包含未经检测的输入路径，允许发送超过缓冲区本身的容量的信息时，就会产生缓冲区溢出。易受攻击的服务可能会导致服务失败，或者允许入侵者获取系统访问权限，危害服务登录帐户的安全上下文。如果此帐户是本地系统或管理员帐户，入侵者可以执行任意的操作，包括控制系统、下载资源、安装恶意软件，以及加载远程控制程序等。

2. 拒绝服务攻击

带有 bug 的服务无法执行正常操作，可以是临时的，也可以是永久的（除非服务重启或是计算机重启）。有时它们会使用复杂的缓冲区溢出攻击，有时则使用单独的网络数据包。例如，旧版本的 Microsoft SQL Server Resolution Service 对 0x04 的 ASCII 码极为敏感。又如，Windows XP SP2 的安全漏洞 Land 攻击就是基于单独的恶意网络数据包。DoS 攻击会阻止合法的服务，并导致进程崩溃、系统资源浪费以及计算机重启等问题。

3. 远程登录访问

许多服务（如 FTP、IIS、远程桌面和终端服务等）提供额外登录点，入侵者能够在这些登录点尝试登录名和密码，试图获取访问权。管理员帐户默认不使用通常帐户的锁定设置。入侵者可以使用登录服务反复尝试管理员密码，既可以手动尝试，也可使用自动密码破解工具。如果没有对安全日志进行监视或及时查看这些安全日志，那么，入侵者的所作所为就很难被发现。

4. 窃听

监听服务之间发送接收数据，入侵者可以截获信息来还原验证信息。许多服务（如 SNMP、Telnet、FTP 和 POP 等）使用明文登录名和密码，即使那些不使用明文数据的服务也有可能受到攻击。例如，RDP 在发行后的一段时间容易受中间人（Man-in-the-Middle，MitM）攻击，即使 RDP 使用加密，新会话也会被截获而传输给远程入侵者。由于在版本 6.0 之前，RDP 不对端点客户端进行验证，就使得 MitM 入侵者有可能深入到通信中，每次获取登录密码的一个字符。许多非法工具使得 RDP MitM 攻击易如反掌，只要入侵者能够进入通信路径就可以。窃听也可以用于捕获登录凭证之外的机密信息和个人信息。

5. 密码泄露

使用从服务登录帐户中列举而得出的密码，入侵者能够提升其在网络中的特权。如果某入侵者具有对某一系统的访问权限（如管理员或本地系统），接下来就会使用各种方法和工具在明文中恢复登录帐户凭据。如果将该凭据应用于其他计算机上，或应用于整个 Windows 域中，就会引起其他资源的泄露。

6. 配置错误

即使一个服务编码完好而且不包含已知弱点，由于用户和管理员经常会错误配置服务，也会使这种服务成为入侵者的工具。例如，用户安装 IIS 或 FTP 服务，却使用了简单的密码。再如，某用户安装了点对点（peer-to-peer）文件共享程序，目的是为了分享文件夹的子目录，但结果却分享了其他所有的硬件驱动器。这些情况都会导致许多机密文件泄露在网络上。

7. 信息泄露

许多服务的系统信息能够被恶意入侵者所利用。信息与服务本身相关，但对服务的正常运行却非常重要，有时恶意连接也会导致信息泄露。

8. 社会工程攻击

与终端用户通信的服务为恶意软件提供了更多途径，如点对点文件共享服务。恶意软件能够与终端用户假装聊天，然后引诱用户接收一个新的文件传输。表面上该文件传输合法的内容和用途，然而却包含着木马恶意软件。许多反恶意软件的程序并不会对其所用服务的内容进行扫描，这样即便是在受保护的计算机上，该病毒也能得以传播。

服务是许多恶意攻击的目标，每增加一种运行的服务，也就相应的扩大了计算机的受攻击面。

11.3 服务强化

在 Blaster 病毒之后，微软建立了 Windows 服务的风险模型，包括更改默认权限和特权、创建新的服务保护措施，因此，在 Windows Vista 之后，服务安全性比以前的操作系统有了很大的改进。其中包括：

- 服务应用最小特权原则；
- 分解服务，更多的服务运行在本地服务和网络服务登录上下文中；
- 为服务分配安全标识符（SID），以便启用服务访问控制；
- 限制特殊服务的 SID；
- 在域中限制服务；
- 所有服务均需会话 0 隔离；
- 所有服务都具有系统强制完整性级别；
- 启用所有服务的数据运行阻止策略；
- 增强 SCM 状态报告。

在接下来的部分会详细阐述以上这些改进的内容。

11.3.1　最小特权

Windows 特权决定安全主体所能执行的操作。换句话说，特权并不是和特定安全对象关联的。Windows Server 2008 包含 35 种不同的特权（如表 11.2 所示），可以指派给不同的安全主体。在“计算机设置\Windows 设置\安全设置\本地策略\用户权利”指派中的组策略，可以看到各种特权，但其中有 9 种权限并不是特权。

表 11.2　默认服务登录帐户特权

特权	本地系统	本地服务	网络服务	管理员	默认用户
AssignPrimaryToken	D	D	D	-	-
SeAudit	E	D	D	-	-
Sebackup	D	-	-	D	-
SeChangeNotify	E	E	E	E	E
SeCreateGlobal	E	E	E	E	E
SeCreatePagefile	E	-	-	D	-
SeCreatePermanent	E	-	-	-	-
SeCreateSymbolicLink	E	-	-	D	-
SeCreateToken	-	-	-	-	-
SeDebug	E	-	-	D	-
SeEnableDelegation	-	-	-	D	-
SeImpersonate	E	E	E	E	E
SeIncreaseBasePriority	E	-	-	D	-
IncreaseQuotaPrivilege	D	D	D	D	-
SeIncreaseWorkingSet	E	E	E	E	E
SeLoadDriver	D	-	-	D	-
SeLockMemory	E	-	-	-	-
SeMachineAccount	-	D	D	D	D
SeManageVolume	D	-	-	D	-
SeProfileSingleProcess	E	-	-	D	-

（续表）

特权	本地系统	本地服务	网络服务	管理员	默认用户
SeRelabel	-	-	-	-	-
SeRemoteShutdown	-	-	-	D	-
SeRestore	D	-	-	D	-
SeSecurity	D	-	-	D	-
SeShutdown	D	-	-	D	-
SeSyncAgent	-	-	-	-	-
SeSystemEnvironment	D	-	-	D	-
SeSystemProfile	E	-	-	D	-
SeSystemtime	D	D	-	D	-
SeTakeOwnership	D	-	-	D	-
SeTcb	E	-	-	-	-
SeTimeZone	E	D	-	D	-
SeTrustedCredManAccess	-	-	-	-	-
SeUndock	D	-	-	D	-
SeUnsolicitedInput	-	-	-	-	-

E=默认启用　D=默认禁用，但是可以启用　-=特权不能启用

本地系统帐户有最多的默认特权，接下来是管理员组的成员，本地服务，网络服务，最后是没有提升特权的普通用户。表 11.2 中包含了所有内置服务帐户，管理员和普通用户的默认特权。

如果服务进程令牌具有特权，但是为禁用的，则其仍然可以启用（因为服务可以启用禁用的特权）。以标准用户运行的进程和在 UAC 中以管理员运行的进程，仅有 5 种默认特权。提升的进程则具有更多的特权。内置管理员帐户和服务登录帐户不属于 UAC。

注意



Windows Vista 和 Windows Server 2008 中的普通用户的权限有所区别。在 Windows Vista 中用户具有 SeTimeZone 特权，即使不是管理员也可以更改系统时区。在 Windows Server 2008 中用户具有创建全局对象特权，共享对象需要该特权，如终端服务以及其他共享服务等。

Microsoft 使用威胁模型分析法分析所有的 Windows 服务。如果某服务不要求本地系统访问权限，则将该服务分配为本地服务或网络服务访问。使用最小特权服务登录帐户，降低了由于服务恶意操作而导致的威胁。尽管只有一半的服务在本地系统环境下运行，但也远远超过了 Windows Server 2003 中的数目。

为了提供更好的保护措施，在 Windows Vista 和 Windows Server 2008 中，在服务启动过程中可以移除任何不必要的默认特权。微软的开发者们对所有默认的 Windows 服务进行了重新设计，移除了所有不必要的特权。于是，许多使用较低权限运行的服务（例如 DHCP 客户端）被分配到其各自的服务登录帐户下。微软提供了许多有用的工具，鼓励开发者分析服务，移除不必要的特权，防止潜在的恶意攻击。在安装服务过程中，服务会安装一个名为 RequiredPrivileges 的注册表项，其中包含服务正常工作所必需的各种特权。

如果一个服务进程（如 Svchost.exe）主控多个服务，SCM 会计算所有服务所需的最小特权的集合，然后移除不必要的特权。当然，如果其中一个服务需要服务登录帐户中所有的特权，

则无需移除特权，而且这些特权可以被所有服务共享。用户可以使用 Sc.exe，其参数为 qprivs，用于查看一个服务所需的特权（不是实际授予进程的特权），语法为：

```
sc.exe<server>qprivs[servicename]
```

例如，在命令提示符窗口中，输入如下命令：

```
sc.qprivs w32time
```

回车执行，显示如图 11.8 所示结果，即可查看 w32time 服务的特权设置。



图 11.8　使用 sc.exe 查看服务特权

用户也可以使用 privs 命令行参数，通过 sc.exe 来查看特权。语法为：

```
sc.<server> privs [Privileges]
```

[Privileges]包含了以/分隔的特权清单，例如，要制定备份和还原特权，可以设置其为 SeBackupPrivilege/SeRestorePrivilege。服务开发者和系统管理员可以利用 SCM 来减小计算机的受攻击面。但是，在更改服务特权前，必须经过合理的分析和测试。

用户还可以使用进程管理器（如图 11.9 所示）查看服务进程特权（以及权限和 SID）。只要是文本框中列出的（已启用或已禁用），都是服务可用的特权。并没有永久的禁用特权，不允许的特权是不会列出来的。

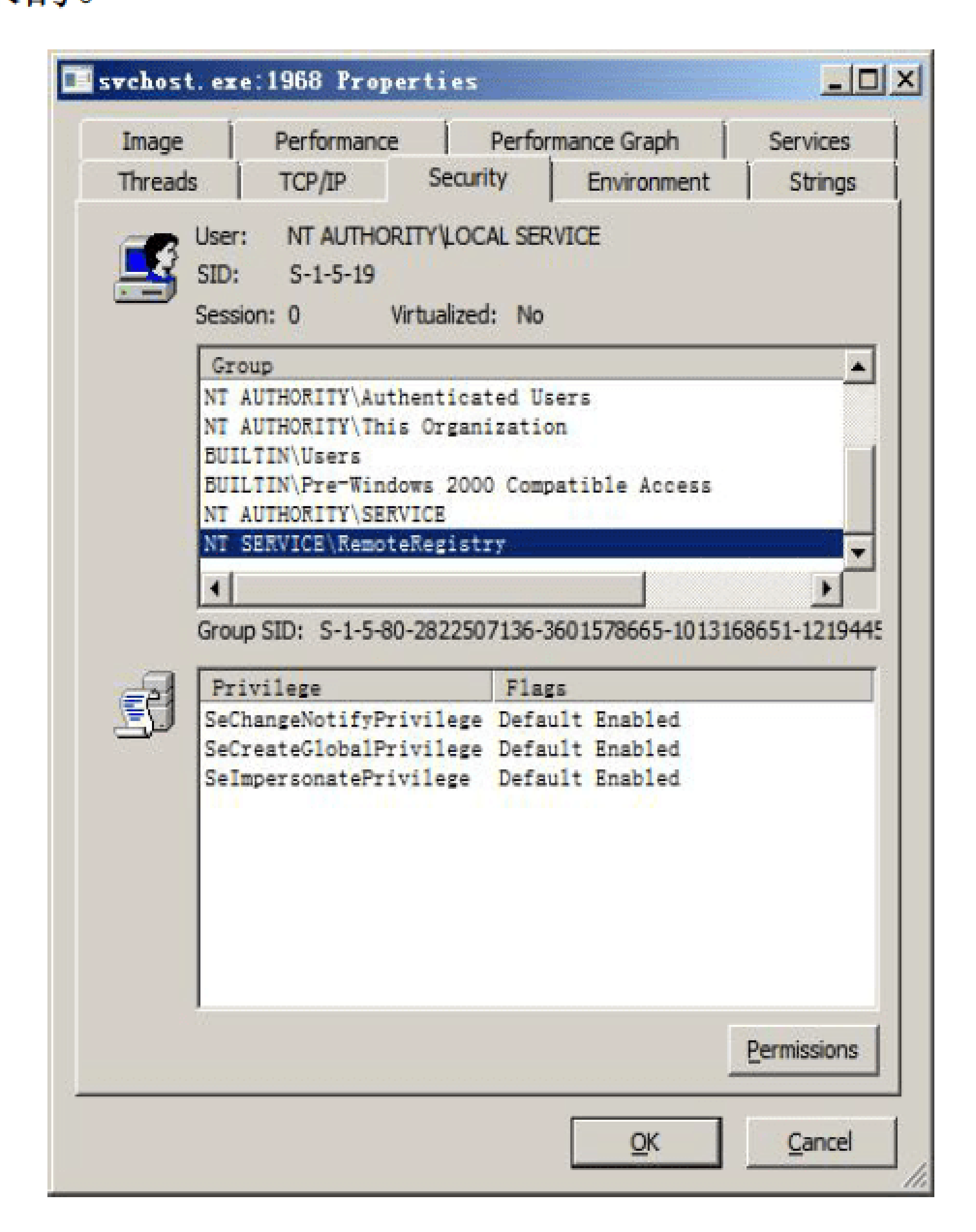


图 11.9　查看服务进程特权

11.3.2　服务 SID

从 Windows Vista 和 Windows Server 2008 开始，每个服务都具有一个特殊的 SID，这个

SID 是基于服务名称的。基于服务的 SID 允许直接为服务指派安全对象的权限，同样也可以用于控制服务，如打开 Windows 防火墙和 IPSec 的端口。

1. 查看服务 SID

管理员可以使用 sc.exe 查看任何服务的 SID，包括并未使用的服务，其语法格式如下：

```
scshowsid [servicename]
```

服务的 SID 是通过其 Unicode 名称计算得出的。使用 SHA-1 加密算法，然后把哈希运算的结果加到 S-1-5-80-之后。例如，服务 W32Time 的 SID 如下：

```
S-1-5-80-4267341169-2882910712-659946508-2704364837-2204554466
```

该 SID 在所有 Windows Vista 和 Windows Server 2008 的操作系统中都是一样的。

若欲赋予服务一个 SID，必须在服务启动之前赋予，并且在服务运行期间不能更改其 SID。这个 SID 会附加在服务的进程令牌上，如果某共享服务进程（例如 Svchost.exe）有多个基于服务的 SID，则所有的 SID 会附加在服务的进程令牌上，供所有共享服务进程中的服务使用。如果某 SID 未被启用，则服务登录帐户的 SID 会附加在服务进程令牌上。

2. 为服务定义访问控制条目

如果某服务令牌有一个服务指定的 SID，就可以定义其许可程序，也可使用 icacls.exe 或其他工具。如图 11.10 所示是一个在 ACL 编辑器中设置权限时，如何查找服务名的例子。必须在服务短名称前加上 NT SERVICE\标签。如图 11.11 所示是在 ACL 编辑器中的结果。虽然必须包含 NT 服务标签来帮助 Windows 查找正确的安全主体，但是使用检查名称按钮，Windows 会将输入的标签转换为服务的短名称（例如 W32Time）。不过，用户无法使用短名称来定义权限。

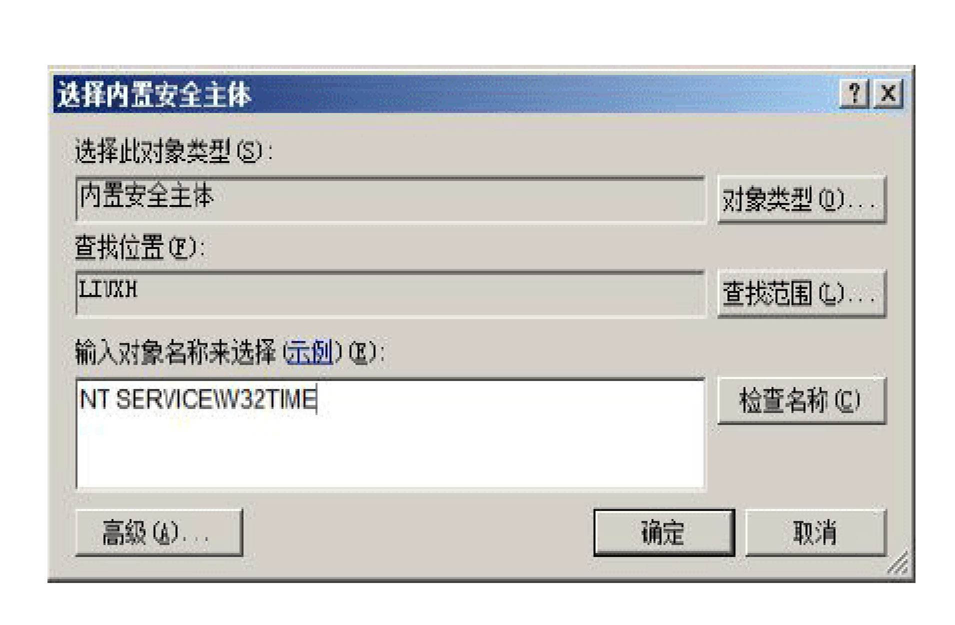


图 11.10　指派 W32Time 服务权限



图 11.11　为 W32Time 服务授予权限

用户可以使用 NT SERVICE\servicename 或服务的 SID 来定义访问控制权限，如图 11.12 所示。


C:\>icacls d:\test2.txt /grant "NT SERVICE\w32time":(d,WDAC)
已处理的文件: d:\test2.txt
已成功处理 1 个文件; 处理 0 个文件时失败

C:\>icacls d:\test2.txt /grant *S-1-5-80-4267341169-2882910712-659946508-2704364837-2204554466:(d,WDAC)
已处理的文件: d:\test2.txt
已成功处理 1 个文件; 处理 0 个文件时失败

C:\>

图 11.12　使用 Icacls.exe 设置服务权限

设置基于服务的 SID 其实非常重要。在 Windows Vista 之前，服务的权限与服务登录帐户的权限是一样的，如果服务登录帐户（例如本地服务）需要具有额外的权限，那么，所有服务也就具有同样的权限了。现在，服务可以允许或是禁止权限。由于服务具有 SID，对象访问审查就会很容易发现服务运行过程中的各种异常。另外，也可以控制服务的网络流量。例如，防火墙默认启用出站筛选，只有特定端口允许服务进行流量交换。

可以使用 sc.exe 查看与服务相关的权限，其语法格式如下：

```
scshowsid [service name] <showrights>
```

输出结果使用 SDDL 转换，增加其他参数可以更加方便的理解访问控制项。使用通常的 Windows 图形用户界面和进程管理器，也可以查看权限设置。

3. 写入受限 SID

服务有 3 种合法的 SID 类型：

- 无（None）;
- 非受限（Unrestricted）;
- 受限（Restricted）。

None 类型表明，该服务没有基于服务的 SID。非受限 SID 指服务有 SID，且该 SID 可以用于访问控制。受限 SID 则表明服务具有额外的访问控制。

当服务被标记为受限时，其自身的 SID 会和下面的 SID 一起，附加到进程令牌的受限 SID 列表中：

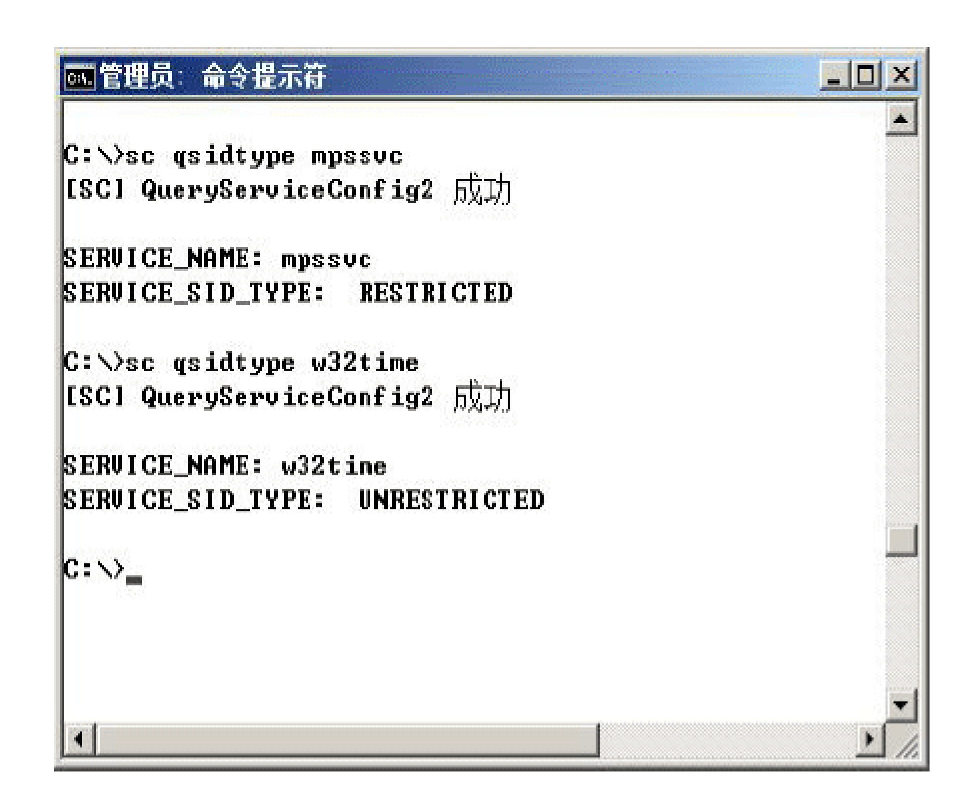
- Everyone SID　(S-1-1-0);
- 登录 SID　(S-1-5-5-0-64163);
- 写入受限 SID　(S-1-5-33)。

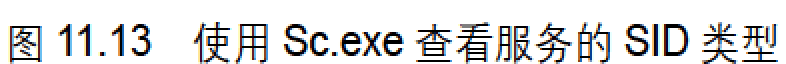
当某个服务尝试对资源进行写操作时，如果其访问令牌含有写入受限 SID，访问就会被拒绝。大多数安全对象不允许 SID 具有写权限，所以系统默认是禁止的。其目的在于，即使恶意软件控制了一个写入受限的服务，那么，所造成的危害也会局限在极小的范围之内。

需要注意的是，只有一部分服务是被标记为写限制的。可以通过 sc.exe 来查看某个服务的 SID 类型，如图 11.13 所示。

写入受限 SID 常常是和防火墙一起使用。防火墙由于自身设计的原因，很容易遭受攻击。Windows 设置了 4 个与之相配套的服务，即 Windows 防火墙（Windows Firewall，MpsSvc）、基本筛选引擎（Base Filtering Engine，Bfe）、诊断策略服务（Diagnostic Policy Service，Dps）和性能日

志与告警（Performance Logs and Alerts，Pla），这都是标记为写限制的服务，包含写限制 SID，如图 11.14 所示。




图 11.13　使用 Sc.exe 查看服务的 SID 类型

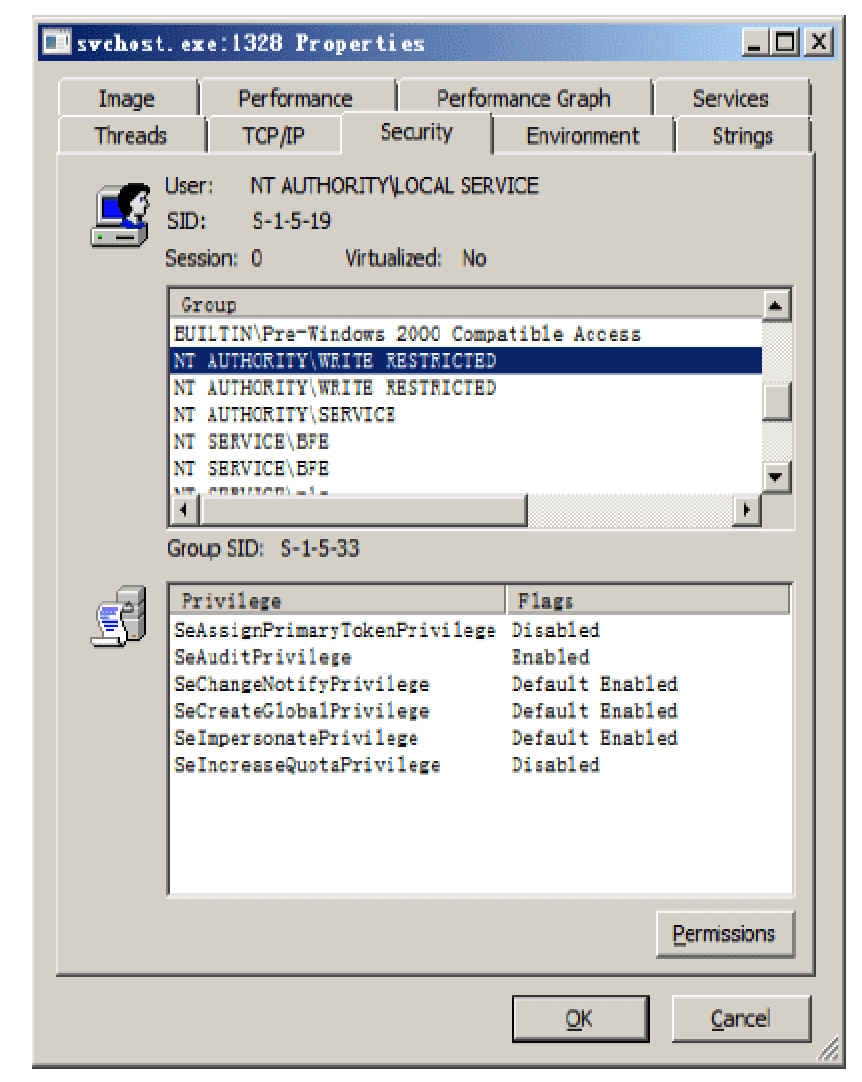


图 11.14　进程管理器显示出某服务的写入受限 SID

在命令提示符窗口中，管理员可以使用如下命令查看对象的写入受限 SID：

```
Icacls /t /findsid "NT AUTHORITY\WRITE RESTRICTED"
```

也可以使用 sc sidtype 命令来设置 SID 类型，其语法格式如下：

```
scsidtype [servicename] <none | restricted | unrestricted>
```

服务启动或是重启动之前，SID 类型的改变并不会起作用。用户和管理员在更改 SID 类型之前，必须要清楚这样做的后果。

注意



受限 SID 比写入受限 SID 还要严格，其既限制读取，也限制写入操作。

---

4. 网络访问受限

管理员可以使用服务名（或 SID）和端口、协议限制，来实现受限网络访问。Windows 高级安全防火墙允许管理员定义文件（公用、专用和域）上的服务。Windows Server 2008 有许多预定义的规则，都是用于服务的。有些规则适用于所有的程序和服务，有些则适用于特定服务，如图 11.15 所示。

Windows Server 2008 默认开启防火墙，同时启用的还有超过 170 个入站（inbound）规则和超过 80 个出站（outbound）规则（如图 11.16 所示）。

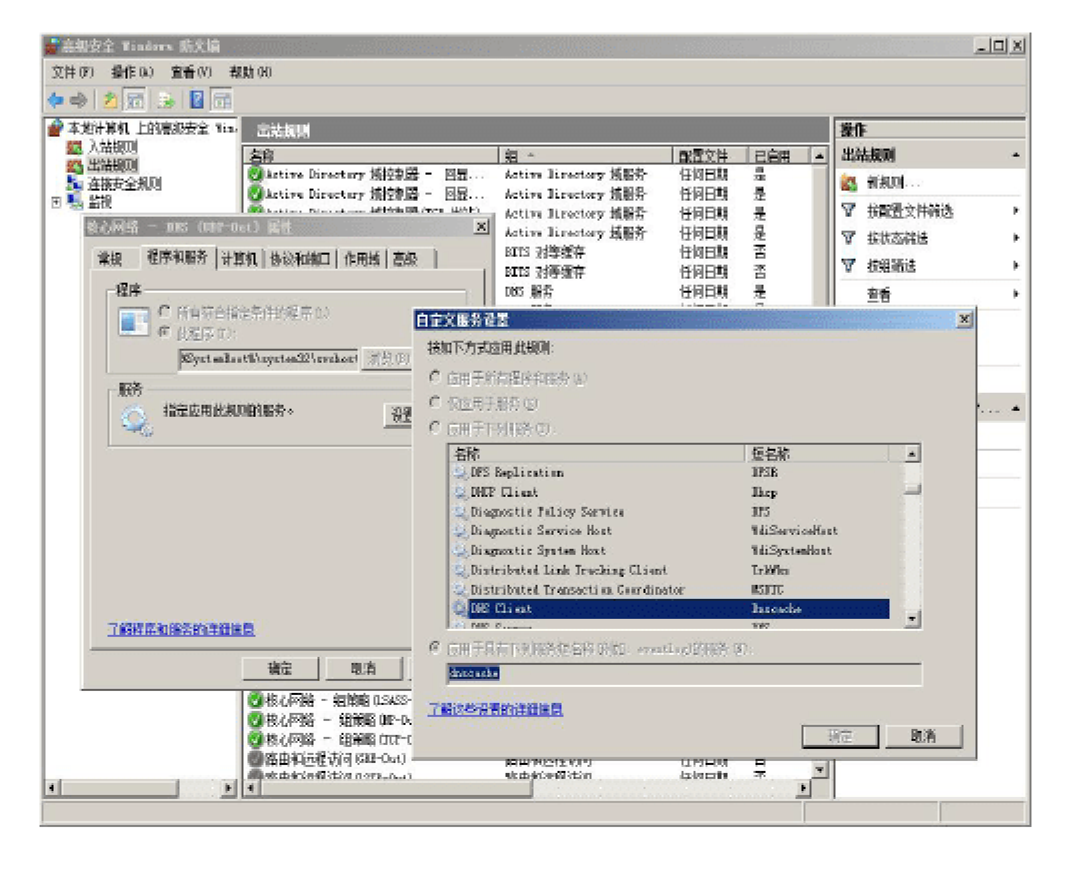


图 11.15 基于服务的防火墙规则

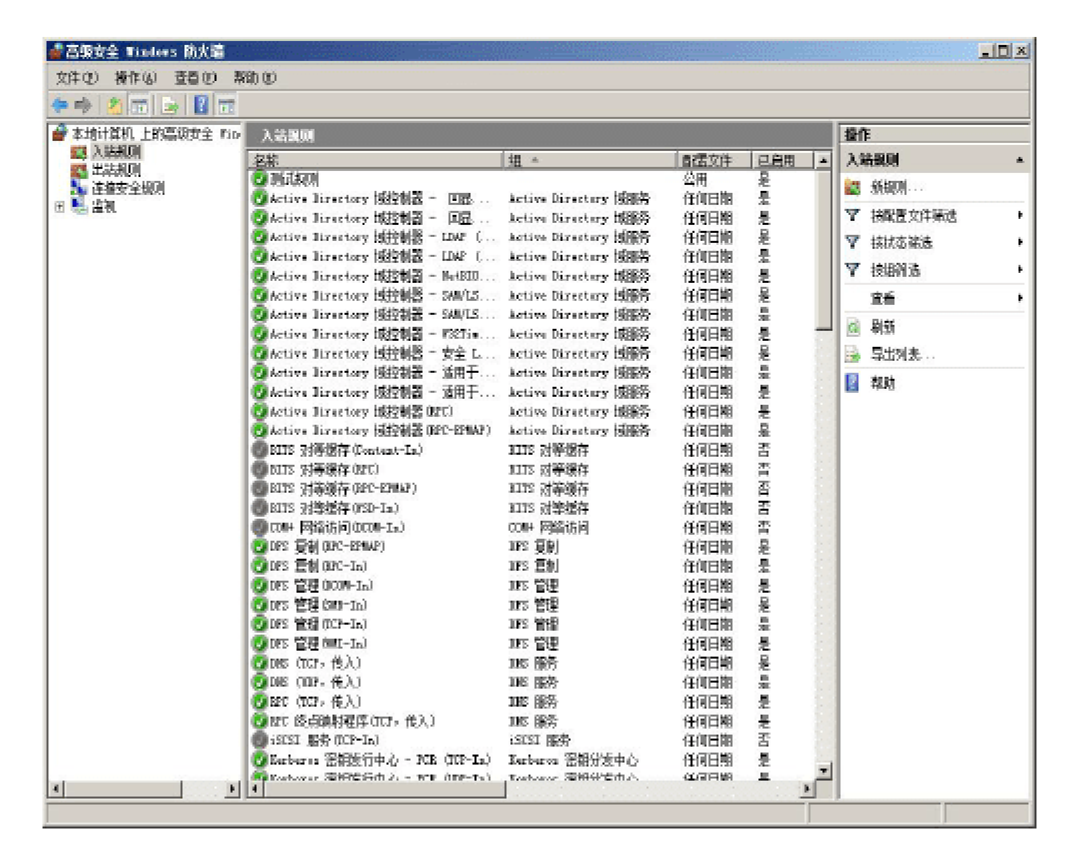


图 11.16 Windows 防火墙保护服务的规则

大多数防火墙规则是针对服务的，每个规则可以是定制或是禁用，管理员也可以增加新的规则。用户可以要求在连接建立前，使用 IPSec 和加密/验证，也可以使用脚本实现规则的设置。Windows Vista 和 Windows Server 2008 包含了超过 80 个预定义发送规则，并且是默认启用的。可以在 HKLM\System\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\RestrictedServices\static 查看这些服务的列表，如图 11.17 所示。

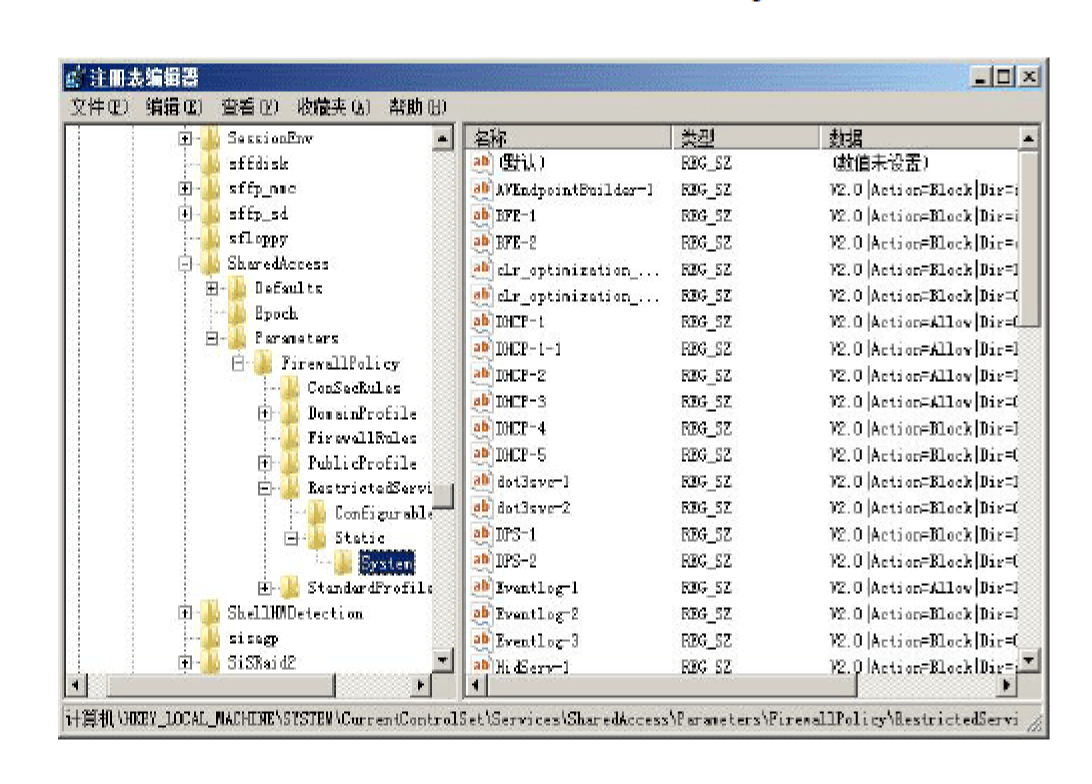


图 11.17 防火墙静态服务规则

这些规则在常规的界面上是看不到的，因为要避免其被修改。如果想要增加规则，应当使用 COM 脚本工具。微软使用域与服务隔离的办法，只能导致网络更加容易受到攻击。某些攻击，包括 Blaster 蠕虫，假如防火墙规则启用的话，当时就不会造成如此巨大的危害。使用防火墙规则，Windows 防火墙可以轻松阻止默认的出站流量。

5. 会话 0 隔离

Windows 中所有的服务都是在会话 0 上运行的，而所有的用户模式应用程序则不是。这可以防止应用程序（可能是恶意程序）在第 0 会话执行。近年来所报告的 Windows 漏洞中，绝大部分与桌面的执行代码有关。所以，服务会话隔离是非常必要的。

会话 0 隔离的缺点是，与终端用户交互的遗留服务无法显示信息和提示。没有垫片的话，遗留服务无法在会话 0 显示信息，终端用户也就不能阅读。交互式服务检测（ui0detect）服务允许遗留服务与终端用户通信。当其启动时（非默认启动），服务会检测试图与用户通信的服务，然后通知登录的交互式用户。据微软消息，UI0detect 服务只是临时垫片，以后将不复存在。软件提供商需要重新编写服务，使其在使用 RPC、COM、命名管道和其他通信方式的会话中与用户沟通。

6. 强制完整性级别

每个服务都有默认的系统强制完整性级别。只有 TrustedInstaller 的完整性级别是高级，

Windows 可以使用 TrustedInstaller 服务来升级、安装和卸载服务。

7. 数据执行保护技术

大多数的服务都是处于数据执行保护（Data Execution Prevention，DEP）和 ASLR 的保护下，如图 11.18 所示。数据执行保护（DEP）通过阻止程序在不可使用的内存执行命令，从而达到解决缓冲区溢出的问题。DEP 和 ASLR 都有助于防范缓冲区溢出，并且还可以阻止某些恶意攻击，其能够抵御之前 Windows 平台所不能防范的攻击。服务的开发者应当确保其服务使用 DEP 和 ASLR。

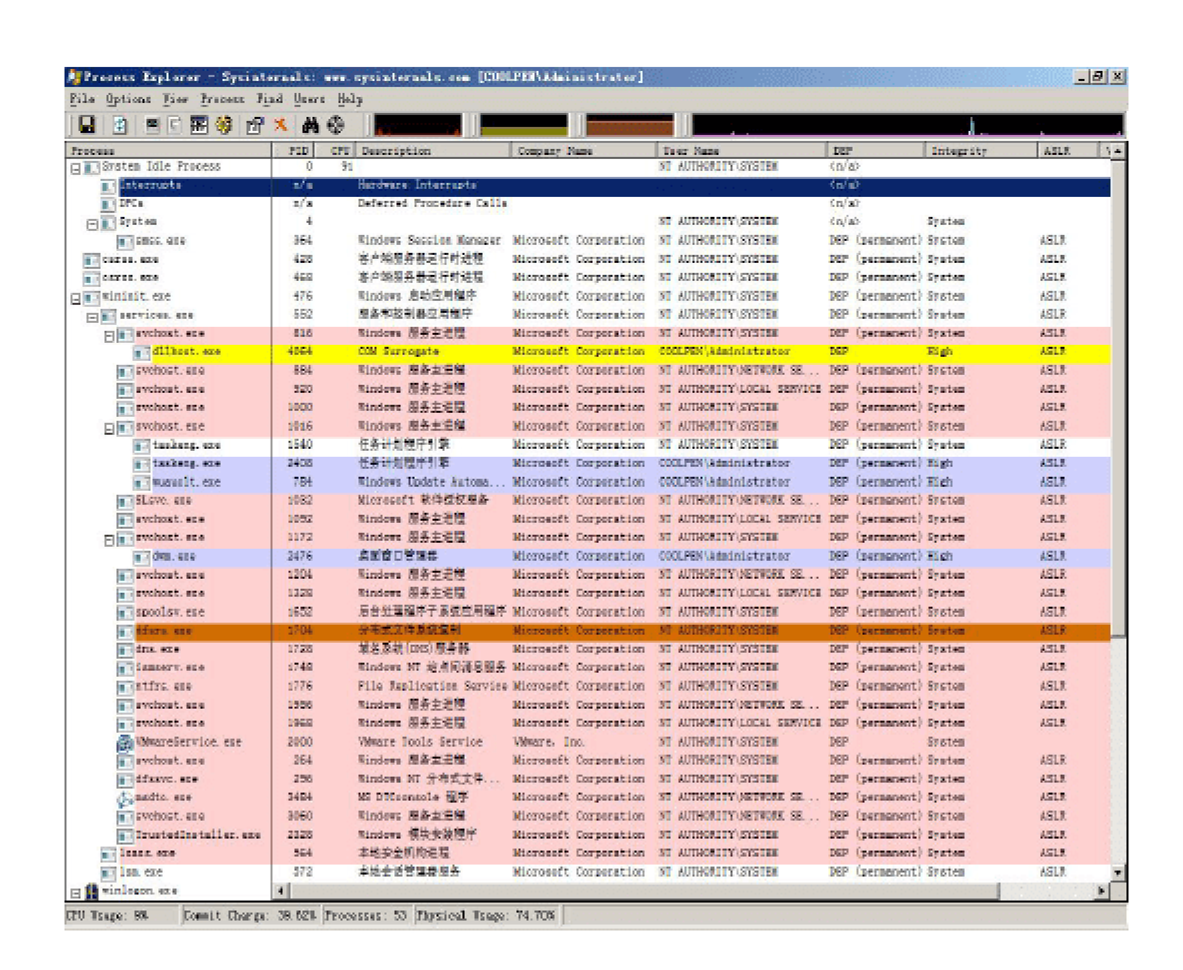


图 11.18 Process Explorer 中的服务

8. 其他 SCM 新特性

在 Windows Vista 之前，客户端只能使用应用程序编程接口（Application Programming Interface，API）、QueryServiceStatusEx 函数以及服务状态登记来确定某服务的状态更改、创建和删除。这种查询方法效率相当低。

Windows Vista 引入了一个新的 API，NotifyServiceStatusChange，其允许 SCM 在服务被创建、删除、状态改变时给客户程序发出通知。这意味着监控服务的程序可以接收服务更改的信息，从而使得开发管理工具更加容易。

在服务关闭之前，其会发出通知，给用户更多的准备时间。关闭服务也考虑到服务的依赖程序，并且关闭服务的顺序也更加合理。

SCM 还可以检测并还原某些非致命错误，在 Windows 的早期版本中，还原操作会导致服务崩溃。现在，内存泄露、系统变慢以及其他问题都进行还原操作。

11.4　服务安全

基于运行服务的风险，微软开发团队分析和改进了所有 Windows 服务的安全性能。虽然如此，作为系统管理员还是应当格外谨慎。以下的这些方法，可以减小被恶意软件侵入的危险。

11.4.1　服务清单

要确保服务安全，管理员必须理解和记录下计算机所需要运行的服务。如果要卸载多余的服务，必须要有服务列表和服务的具体说明。很多内置和第三方工具可以提供这个列表，例如 Sc.exe，其可以用来查询本地和远程服务，然后返回服务信息（特权、状态、启动类型等），

供管理员参考。Windows 管理规范（Windows Management Instrumentation，WMI）和 Windows 管理规范命令行（Windows Management Instrumentation Command-line，WMIC）也可以做到，例如，要查询 Server1 上的服务信息，可以在命令提示符窗口中，输入如下命令：

```
wmic /output:c:\services.htm /node:server1 service list full / format:htable
```

回车执行，显示如图 11.19 所示结果。

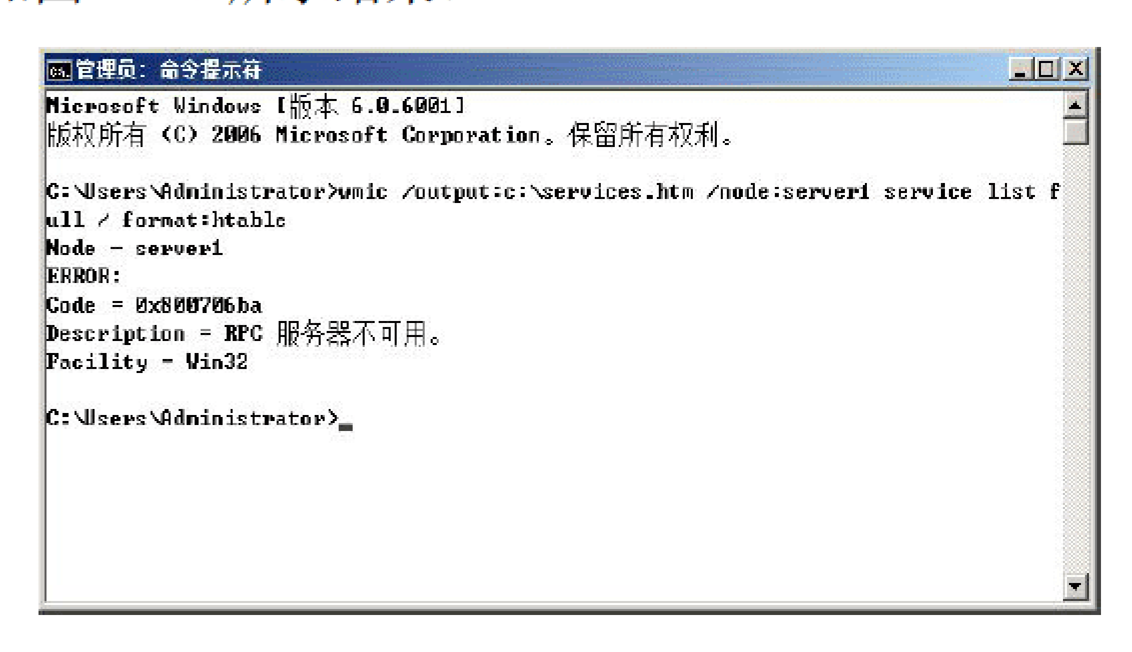


图 11.19　要查询 Server1 上的服务信息

使用 Internet Explorer 可以检查 C:\services.htm file，其他工具，例如系统管理服务器或系统中心设置管理器，都可以用来返回详尽的服务清单。应当根据企业的风险接受级别、周期性查看服务清单。如果不能确定计算机系统的服务清单，应当首先启动风险接受级别最高的系统及与其相关的系统。

11.4.2　最小化运行服务

首先确认哪些是必需的服务，然后卸载或禁用多余的服务，这是非常必要的。运行的服务越少，服务器就越不容易受到攻击。通常情况下，系统所启用的服务，都是某些角色必需的，而对于明显多于的服务和不符合企业策略的服务，用户可以根据需要修改。以 DHCP 客户端为例，许多服务器，包括有静态地址的服务器，都默认启用 DHCP 客户端，这可能导致未经授权的对等文件共享。如果系统中有许多未经授权的潜在危险服务，管理员在检测系统时会发现这些问题的。

如果用户想要对默认服务进行修改，建议用户操作之前咨询一下专业人士。Windows Vista 和 Windows Server 2008 中服务的介绍以及相关建议，用户可以参考如下网址：

- http://www.microsoft.com/whdc/system/vista/Vista_Services.mspx
- http://www.microsoft.com/downloads/details.aspx?FamilyID=a3d1bbed-7f35-4e72-bfb5-b84a526c1565&displaylang=en
- http://www.microsoft.com/downloads/details.aspx?FamilyID=fb8b981f-227c-4af11-a44b-b115696a80ac&DisplayLang=en

多余的服务应当予以卸载或是禁用。卸载比较安全，不过禁用的话还可以在日后需要时再启用。另外，在禁用或是卸载服务之前，必须要弄清楚这样做的后果。经常备份系统，是一个

好习惯，即便修改服务出现了问题，也可以亡羊补牢。

11.4.3 使用最小化特权安全模型

微软已经对所有的服务实行了最小化特权原则。最小化特权安全模型更多的用于第三方或用户定义的服务。不过，很多软件供应商对最小化特权都不是很感兴趣，尤其是服务的最小化特权安全模型。

如果安装了新的服务，但不熟悉其安全级别，应当咨询软件提供商。使用 Sc.exe 可以查看服务的 SID、SID 类型、登录帐户和所需特权等信息。如果特权和权限超过了服务应得的级别，需要联系软件提供商，并请求最小化特权协助。如果软件提供商不支持最小特权原则，最好是卸载这个服务。对于软件提供商来说，最重要的是顾客的反应及其对产品的支持。

11.4.4 及时更新

微软提供软件升级，可以修补系统漏洞，提高安全性，并且优化性能。如果服务有致命性的 bug，并且影响到很大的用户群，微软的反应就会非常迅速，立刻会提供相应的补丁下载。及时升级，是增强安全的必要措施。历史上最危险的两种恶意软件（SQL Slammer 和 Blaster）都是针对未能及时更新的计算机。

11.4.5 创建和使用自定义服务帐户

微软建议尽可能使用内置服务帐户（本地系统、本地服务和网络服务），不过，创建自定义服务登录帐户在某些时候更能达到安全的目的。

1. 使用高强度密码并定期更换

自定义服务登录帐户应当有一个高强度的密码，并且定期更换。自定义服务帐户在两个地方存储密码：本地 SAM 数据库的动态目录和本地系统中可检索并使用 SCM 的目录中。当更改密码时，这两个地方的密码都会随之更改。虽然这样做有点麻烦，但是其能够保证帐户的安全。使用脚本可以简化此操作，包括 Microsoft Developer Network 提供的一个脚本。

注意



使用密码检查工具，检查登录帐户密码的弱点，以便及时更换密码。

2. 使用组策略

如果使用高特权的自定义服务登录帐户，应用组策略可以简化权限分配的工作，同时也可以避免权限的误用。当组和其成员属于受限组（计算机配置\策略\Windows 设置\安全设置\受限组）时，对于受限制的组特性之外的修改是无效的。自定义服务登录帐户的特权和权限可以

指派给组，组成员则会强制使用受限组。

3. 尽量少使用域管理员帐户

不要在非域控制器上使用域管理员组的自定义服务登录帐户，否则一旦出现问题的话，整个森林都会被波及。使用其他帐户，比如本地系统帐户，看看能不能被服务所接受。在使用高特权级别服务帐户时，一定要注意这点。

4. 使用本地系统帐户

很多专家建议说，如果可以的话，应当把需要本地系统访问权限的服务都转移到较低的自定义服务帐户上去。有的管理员就此得出结论，认为要尽量避免运行本地系统中的服务。这样的想法完全忽略了本地系统帐户所提供的保护机能。因为本地帐户没有密码，入侵者也就无从下手。如果入侵者攻击在本地系统上下文中运行的服务，其只能控制本地计算机，而无法入侵域和森林中的计算机，除非他获得了域管理员帐户。

使用服务，最好是使用最小特权的服务登录帐户，尽量使用本地服务或网络服务，如果不需要管理员或本地系统权限，应当创建自定义最小化特权的服务帐户。如果软件提供商认为，其服务必须要在非域控制器的域管理员上下文中运行，则应当使用自定义服务帐户，允许服务具有其需要访问资源的完全管理权限。更彻底的做法是，将产品退货并要求退款。重要文件和注册表资源的完全控制权限，比域管理员组的帐户还要重要。大多数文件和文件夹的完全控制权限，如果指派给非管理员组，则服务不能添加和移除用户、更改用户密码以及进行其他管理操作。系统的完全控制权限和管理员访问权限并不一样。如果服务帐户不需要管理员权限，应授予其本地系统权限。本地系统是本地管理员，无需定期更改密码。

小　　结

Windows Server 2008 和 Windows Vista 上的服务，比起之前版本的操作系统，已经有了很大改善。通过应用最小特权原则、隔离会话 0、限制网络访问以及使用 DEP 和 ASLR 保护，服务的运行更加安全。管理员可以移除不必要的服务，应用最小特权模型，从而降低系统面临的安全风险。虽然 Windows 一直是入侵者的攻击目标，但是最小特权服务能提供有效的保护。

习　　题

1. 简述何为系统服务安全。
2. 介绍几种最普通的攻击威胁。

实验：配置系统服务安全

实验目的

掌握如何配置系统服务，以及服务的启动与停止的不同方法。

实验内容

配置 DHCP Client 服务的启动类型为“自动”。使用图形界面停止该服务，然后使用命令方式重新启动服务。

实验步骤

1. 设置服务的启动方式。
2. 使用图形界面停止该服务。
3. 使用 net start 命令重新启动服务。

第12章

端口安全

端口也称“网络接口”，是服务器上的网络服务对外提供的主要通道，一台被配置 IP 地址的服务器，可以提供多种不同的网络服务。许多网络攻击都是从常用端口扫描开始的，通过扫描远程计算机端口发现漏洞进而攻击，所以计算机端口对每个计算机用户来说非常重要。通常不使用默认端口，并且关闭不需要的端口，以减少被攻击的机率。

本章导读

- 端口介绍
- 扫描端口
- 查看端口
- 关闭端口
- 重定向默认端口

12.1 端口介绍

众所周知，计算机之间通信是通过端口进行的，当要访问一个网站时，Windows 会在本机开一个端口，然后去连接远方网站服务器的一个端口，当其他主机访问本地计算机时也是如此。默认状态下，Windows 会在计算机上打开许多服务端口，黑客常常利用这些端口来实施入侵，因此掌握端口方面的知识，是安全上网必备的技能。

12.1.1 端口概述

“端口”，可以认为是计算机与外界通讯交流的出入口。在硬件领域的端口又称接口，如：USB 端口、串行端口等。在软件领域的端口一般是指网络中面向连接服务和无连接服务的通信协议端口，是一种抽象的软件结构，包括一些数据结构和 I/O 缓冲区。

在网络技术中，“端口”有好几种含义。集线器、交换机采用路由器的端口指的是连接其他网络设备的接口，如 RJ-45 端口、Serial 端口等。而这里所指的端口不是指物理意义上的端口，而是特指 TCP/IP 协议中的端口，是逻辑意义上的端口。

12.1.2 端口的分类

每个 IP 地址可提供 65 536 个端口，想详细记住每个端口的功能、状态、类型等详细信息，显然是不太可能的。为了便于应用和管理，管理员需要了解一些常用的端口分类方式。从逻辑意义上说，端口分类有多种分类标准，按端口号分布划分和按协议类型划分是其中较为常用的两种分类方法。

1. 按端口号划分

按照端口号划分，可以将端口分为 3 大类，即公认端口、注册端口、动态或私有端口。

（1）公认端口

公认端口（Well Known Ports）范围为 0~1 023。这些端口号一般被系统固定地分配给了一些服务。例如 21 端口被分配给 FTP 服务，25 端口被分配给 SMTP（简单邮件传输协议）服务，110 端口被分配给 POP3 服务，80 端口被分配给 WWW 服务，135 端口被分配给 RPC（远程过程调用）服务等。

（2）注册端口

注册端口（Registered Ports）范围为 1 024~49 151。注册端口松散绑定于一些服务，即端口号一般不会固定分配给某个服务，许多服务都可以使用这些端口。只要运行的程序向系统提

出访问网络的申请，那么，系统就可以从这些端口号中，自动分配一个端口供程序使用。比如，1 024 端口分配给第一个向系统发出申请的程序，而在该程序进程关闭后，就会释放其所占用的 1 024 端口。因此，注册端口在一定程度上降低了系统的安全性。

（3）动态或私有端口

动态或私有端口（Dynamic and/or Private Ports）范围为 49 512~65 535。通常情况下，不建议为服务分配这些端口。动态端口和注册端口并无太大区别，因此可以直接将端口按照端口号划分为公认端口（0~ 1 023）和私有端口（1 024~65 535）。

2. 协议类型划分

端口按协议类型划分，可以分为 TCP、UDP 等端口。

（1）TCP 端口

TCP 端口是由 TCP 协议而来的，即传输控制协议端口，需要在客户端和服务器之间建立连接，这样可以提供可靠的数据传输。

常用 TCP 端口包括：

- HTTP：超文本传送协议使用 80 端口，用于实现 Web 服务和网页浏览；
- FTP：文件传输协议使用 21 端口，用于实现文件的上传和下载；
- SMTP：简单邮件传送协议使用 25 端口，用于发送电子邮件；
- POP3：邮局协议使用 110 端口，用于接收电子邮件。

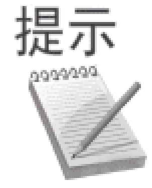
（2）UDP 端口

UDP 端口，即用户数据包协议端口，无需在客户端和服务器之间建立连接，安全性得不到保障。常见的有 DNS 服务的 53 端口、SNMP（简单网络管理协议）服务的 161 端口、QQ 使用的 8 000 和 4 000 端口等。

常用 UDP 端口包括：

- DNS：域名解析服务使用 53 端口，用于实现将域名解析为 IP 地址；

提示



DNS 服务还同时使用 TCP 53 端口。

- SNMP：简单网络管理协议使用 161 端口，用于实现对网络设备的远程管理和监视，由于网络设备很多，所以无连接的服务体现出其优势；
- QQ：QQ 服务使用 8 000 端口，监听是否有信息发送过来，客户端使用的则是 4 000 端口，并通过该端口向外发送信息，但如果上述端口正在使用（例如，同时与几个好友聊天），则端口号顺序自动递增 4 001、4 002。

12.1.3 应用程序和服务端口

任何网络应用都离不开端口，大多数应用程序和服务都使用固定的公认端口，因此使用过程中可以省略端口标识。虽然方便了应用，但同时也为入侵者留下了“后门”。为了提高系统和网络通信的安全，用户必须掌握常用应用程序和服务使用的端口，以便在必要时对其进行配置。如表 12.1 所示为 Windows 服务器和常见应用程序所使用的端口号及端口类型。

表 12.1 常见应用程序和服务端口

端口号	端口类型	应用或服务
7	TCP/UDP	回显协议 Echo
23	TCP	Telnet 协议
25	TCP	简单邮件传输协议(SMTP)
43	TCP	别名/Whois 协议
53	TCP/UDP	域名系统协议(DNS)
67	UDP	DHCP(请求)
68	UDP	DHCP(答复)
69	UDP	普通文件传输协议(TFTP)
80	TCP	超文本传输协议(HTTP)
110	TCP	邮局协议 v.3(POP3)
135	TCP	用于发布 Exchange 服务器从外部网络访问 RPC
135	TCP	远程过程调用协议 RPC
137	UDP	NetBIOS 名称服务协议
138	UDP	NetBIOS 数据报协议
139	TCP	NetBIOS 会话协议
143	TCP	交互式的邮件访问(IMAP4)
389	TCP/UDP	轻型目录访问协议(LDAP)
443	TCP	安全超文本传输协议(HTTPS)
1 433	TCP/UDP	Microsoft SQL
1 863	TCP	MSN 即时消息协议（MSN 即时消息协议）
5 190	TCP	AOL 即时消息协议
5 190	TCP	ICQ 2000 协议
5 500	UDP	SecurID
6 667	TCP	Internet 中继聊天(IRC)
6 801	UDP	Net2Phone 协议（辅助 TCP 3 000~4 000, TCP 7 800~7 900）
7 070	TCP	Progressive Networks 流媒体协议(PNM)
8 000	UDP	QQ 即时信息

12.2　端口扫描

一个端口就是一个潜在的通信通道，也是一个入侵通道。对目标计算机进行端口扫描，能得到许多有用的信息。进行扫描的方法很多，可以手工进行扫描，也可以用端口扫描软件进行扫描。在手工进行扫描时，需要熟悉各种命令。对命令执行后的输出进行分析。用扫描软件进行扫描时，许多扫描器软件都有分析数据的功能。通过端口扫描，可以得到许多有用的信息，从而发现系统的安全漏洞。

12.2.1　端口扫描原理

扫描器是一种自动检测远程或本地主机安全性弱点的程序,通过使用扫描器用户可以不留痕迹的发现远程服务器的各种 TCP 端口的分配及提供服务的情况，这就能使得用户间接或直观了解到远程主机所存在的安全问题。

扫描器通过选用远程 TCP/IP 不同的端口服务，记录目标给予的回答，通过此类方法，可以搜集到很多关于目标主机各种有用的信息。

12.2.2　端口扫描应用

扫描器并不是一个直接攻击网络漏洞的程序，只能帮助用户发现目标主机某些内在的弱点。一个好的扫描器能对其得到的数据进行分析，帮助用户查找目标主机的漏洞，却不会提供进入一个系统的详细步骤。

扫描器应该有三项功能：

- 发现一个主机或网络的能力；
- 发现什么服务正运行在这台主机上的能力；
- 通过测试这些服务，发现漏洞的能力。

12.2.3　端口扫描技术

当确定了目标主机可达后，可以使用端口扫描技术，发现目标主机的开放端口，包括网络协议和各种应用监听的端口。端口扫描技术主要包括以下三类：

- 开放扫描：会产生大量的审计数据，容易被对方发现，但其可靠性高；
- 隐蔽扫描：能有效的避免对方入侵检测系统和防火墙的检测，但这种扫描使用的数据包在通过网络时容易被丢弃从而产生错误的探测信息；
- 半开放扫描：隐蔽性和可靠性介于前两者之间。

1. TCP connect（）扫描

TCP connect（）扫描是最基本的 TCP 扫描。connect（）是一种系统调用，由操作系统提供，用来与每一个感兴趣的目标计算机的端口进行连接。如果目标端口有程序监听状态，connect（）就会成功返回，否则这个端口是不可用的，即没有提供服务。

这个技术的一个最大的优点是，系统中的任何用户都有权利使用这个调用。另一个优点就是速度。如果对每个目标端口以线性的方式，使用单独的 connect（）调用，那么将会花费相当长的时间，用户可以通过同时打开多个套接字，从而加速扫描。使用非阻塞 I/O 允许用户设置一个低的时间用尽周期，同时观察多个套接字。此类方法的缺点非常容易被发觉，且被过滤掉。目标计算机的 logs 文件会显示一连串的连接和连接出错的服务消息，并且在很短的时间内将其它关闭。

2. TCP SYN 扫描

扫描器向目标主机端口发送 SYN 包。如果应答是 RST 包，那么说明端口是关闭的；如果应答中包含 SYN 和 ACK 包，说明目标端口处于监听状态，再传送一个 RST 包给目标机从而停止建立连接。由于在 SYN 扫描时，全连接尚未建立，所以这种技术通常被称为半连接扫描，其优点和缺点如下：

- 优点：隐蔽性较全连接扫描好，一般系统对这种半扫描很少记录；
- 缺点：通常构造 SYN 数据包需要超级用户或者授权用户访问专门的系统调用。

3. TCP FIN 扫描

扫描器向目标主机端口发送 FIN 包。当一个 FIN 数据包到达一个关闭的端口，数据包会被丢掉，并且返回一个 RST 数据包。否则，若是打开的端口，数据包只是简单的丢掉（不返回 RST）。

- 优点：由于这种技术不包含标准的 TCP 三次握手协议的任何部分，所以无法被记录下来，从而必 SYN 扫描隐蔽得多，FIN 数据包能够通过只监测 SYN 包的包过滤器。
- 缺点：
  - 跟 SYN 扫描类似，需要自己构造数据包，要求由超级用户或者授权用户访问专门的系统调用；
  - 通常适用于 UNIX 目标主机，除过少量的应当丢弃数据包却发送 RST 包的操作系统（包括 CISCO，HP/UX，MVS 和 IRIX）。但在 Windows95/NT 环境下，该方法无效，因为不论目标端口是否打开，操作系统都返回 RST 包。

4. IP 段扫描

IP 段扫描不算是一种新方法，只是其技术在不断变化。IP 段扫描并不是直接发送 TCP 探测数据包，是将数据包分成两个较小的 IP 段。这样就可以将一个 TCP 头分成好几个数据包，从而过滤器就很难探测到。

5. TCP 反向 ident 扫描

ident 协议允许看到通过 TCP 连接的任何进程的拥有者的用户名，即使这个连接不是由这个进程开始的。例如，连接到 http 端口，然后用 Ident 来发现服务器是否正在以 root 权限运行。其缺点就是使用这种方法只能在和目标端口建立了一个完整的 TCP 连接后才能看到。

6. FTP 返回攻击

FTP 协议的特点是支持代理 FTP 连接。即入侵者可以从本地计算机 src.com 和目标主机 dest.com 的 FTP server-PI（协议解释器）连接，建立一个控制通信连接。然后，请求这个 server-PI 激活一个有效的 server-DTP（数据传输进程）用来给 Internet 上任何地方发送文件。对于一个 User-DTP，尽管 RFC 明确定义，请求一个服务器发送文件到另一个服务器是可以的，但是对于目前的大多数用户并不支持。

利用 FTP 返回攻击的目的是从一个代理的 FTP 服务器来扫描 TCP 端口。这样，用户能在一个防火墙后面连接到一个 FTP 服务器，然后扫描端口。如果 FTP 服务器允许从一个目录读写数据，用户就能发送任意的数据到发现的打开的端口。对于端口扫描，这个技术是使用 PORT 命令来表示被动的 User DTP 正在目标计算机上的某个端口监听。然后入侵者试图用 LIST 命令列出当前目录，结果通过 Server-DIP 发送出去。如果目标主机正在某个端口监听，传输就会成功，否则，就会出现“425 Can't build data connection:Connection refused.”。然后，使用另一个 PORT 命令，尝试目标计算机上的下一个端口。这种方法的优点很明显，难以跟踪，能穿过防火墙。主要缺点是速度很慢，有的 FTP 服务器最终能得到一些线索，关闭代理功能。

7. UDP ICMP 端口不能到达扫描

这种方法与上面几种方法的不同之处在于使用的是 UDP 协议。由于这个协议很简单，所以扫描变得相对比较困难。这是由于打开的端口对扫描探测并不发送一个确认，关闭的端口也并不需要发送一个错误数据包。幸运的是，许多主机在用户向一个未打开的 UDP 端口发送一个数据包时，会返回一个 ICMP_PORT_UNREACH 错误。这样用户就能发现哪个端口是关闭的。UDP 和 ICMP 错误都不保证能到达，因此这种扫描器必须还实现在一个包看上去是丢失的时候能重新传输。这种扫描方法是很慢的，因为 RFC 对 ICMP 错误消息的产生速率做了规定。

8. UDP recvfrom（）和 write（） 扫描

当非 root 用户不能直接读到端口而不能到达错误时，操作系统能间接地在它们到达时通知用户。比如，对一个关闭的端口的第二个 write（）调用将失败。在非阻塞的 UDP 套接字上调用 recvfrom（）时，如果 ICMP 出错还没有到达时返回“EAGAIN-重试”。如果 ICMP 到达时，返回“ECONNREFUSED-连接被拒绝”。这就是用来查看端口是否打开的技术。

9. ICMP echo 扫描

ping 的实现机制，在判断在一个网络上主机是否开机时非常有用。向目标主机发送 ICMP Echo Request（type 8）数据包，等待回复的 ICMP Echo Reply 包。如果能收到，则表明目标系统可达，否则表明目标系统已经不可达或发送的包被对方的设备过滤掉。其优点是简单，系统支持，然而缺点却是容易被防火墙限制。

12.3　查看端口

在局域网使用时，常常会发现系统中开放了一些莫名其妙的端口；在系统运行应用程序和网络服务时，端口状态也可能在不断变化，并且有些应用程序可能会同时调用多个端口，总体来说，给系统的安全带来了隐患。为了让端口的使用情况尽在掌握之中，需要了解当前端口的开放情况和工作状态，为此，可以通过 netstat 命令和第三方工具检查出使用端口的特定程序。

12.3.1　使用 netstat 命令查看端口

只要用户为本地计算机网卡正确安装了 TCP/IP 协议，就可以使用 Windows 提供的 netstat 命令，来查看本地计算机的端口开放情况。在 Windows Server 2008 系统中，TCP/IP 协议是默认安装的，所以用户无需任何操作即可使用该工具。

netstat 用于显示与 IP、TCP、UDP 和 ICMP 协议相关的统计数据，一般用于检验本机各端口的网络连接情况。

01 依次选择“开始”→“所有程序”→“附件”→“命令提示符”命令，右击该选项，在弹出的快捷菜单中选择“以管理员身份运行”命令。打开“管理员：命令提示符”窗口。

02 在该窗口中，输入“netstat an”命令，按下回车键，显示如图 12.1 所示结果。

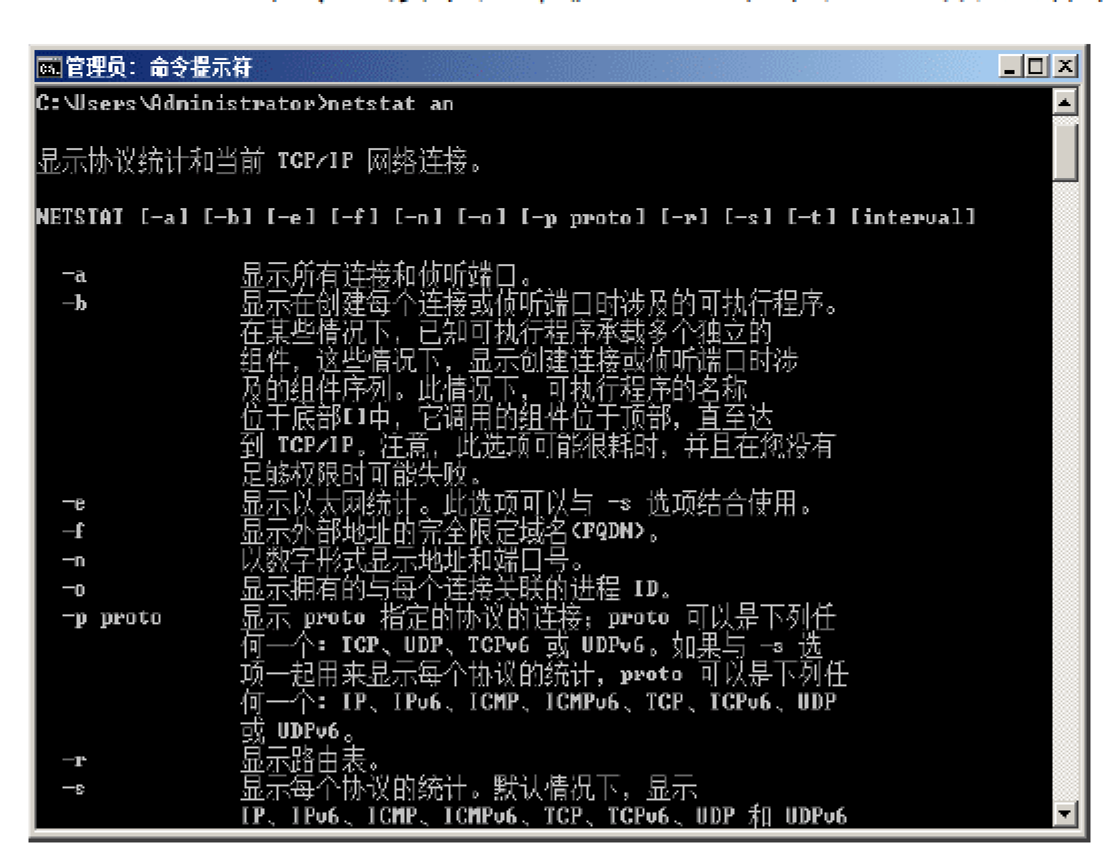


图 12.1　“netstat an”命令窗口

语法：netstat[-a][-b] [-e] [-f][-n] [-o] [-p proto] [-r] [-s][-t] [interval]

参数如下：

- -a 显示所有连接和监听端口；
- -b 显示在创建每个连接或监听端口时涉及的可执行程序。在某些情况下，已知可执行程序承载多个独立的组件，这些情况下，显示创建连接或监听端口时涉及的组件序列。此情况下，可执行程序的名称位于底部[ ]中，它调用的组件位于顶部，直至达到 TCP/IP。注意，此选项可能很耗时，并且在没有足够权限时可能失败；

- -e 显示以太网统计。该参数可以与-s 选项结合使用；
- -f 显示外部地址的完全限定域名<FQDN>；
- -n 以数字形式显示地址和端口号；
- -o 显示拥有的与每个连接关联的进程 ID；
- -p proto 显示 proto 指定的协议的连接；proto 可以是下列任何一个：TCP、UDP、TCPv6 或 UDPv6。如果与-s 选项一起用来显示每个协议的统计，proto 可以是下列任何一个：IP、IPv6、ICMP、ICMPv6、TCP、TCPv6、UDP 或 UDPv6；
- -r 显示路由表；
- -s 显示每个协议的统计。默认情况下，显示 IP、IPv6、ICMP、ICMPv6、TCP、TCPv6、UDP 和 UDPv6 的统计。-p 选项可用于指定默认的子网；
- -t 显示当前连接卸载状态；
- Interval 重新显示选定的统计，各个显示间暂停的隔秒数。按 Ctrl+C 停止重新显示统计。如果省略，则 netstat 将打印当前的配置信息一次。

---

1. netstat -a

显示本地计算机上所有连接和监听的端口。在“管理员：命令提示符”窗口中，输入“netstat -a”命令，按下回车键。显示如图 12.2 所示。

```
管理员: 命令提示符
  TCP    [::]:135              zmj-2008:0          LISTENING
  TCP    [::]:445              zmj-2008:0          LISTENING
  TCP    [::]:2009             zmj-2008:0          LISTENING
  TCP    [::]:5357             zmj-2008:0          LISTENING
  TCP    [::]:49152            zmj-2008:0          LISTENING
  TCP    [::]:49153            zmj-2008:0          LISTENING
  TCP    [::]:49154            zmj-2008:0          LISTENING
  TCP    [::]:49155            zmj-2008:0          LISTENING
  TCP    [::]:49156            zmj-2008:0          LISTENING
  UDP    0.0.0.0:123           *:*
  UDP    0.0.0.0:500           *:*
  UDP    0.0.0.0:3702          *:*
  UDP    0.0.0.0:3702          *:*
  UDP    0.0.0.0:4500          *:*
  UDP    0.0.0.0:5355          *:*
  UDP    0.0.0.0:62856         *:*
  UDP    192.168.1.116:137     *:*
  UDP    192.168.1.116:138     *:*
  UDP    [::]:123              *:*
  UDP    [::]:500              *:*
  UDP    [::]:3702             *:*
  UDP    [::]:3702             *:*
  UDP    [::]:5355             *:*
  UDP    [::]:62857            *:*

C:\Users\Administrator>
```

图 12.2　“netstat -a”命令窗口

提示　LISTENING 都表示该端口是处于开放状态，是可以连接的；ESTABLISHED 则表示该端口处于被连接状态。

---

2. netstat -an

查看当前有哪些计算机正在与本机连接，并且所使用的 IP 地址以及端口等信息，如果想要达到这个目的，可以使用此命令进行查看。

在“管理员：命令提示符”窗口中，输入“netstat -an”命令，按下回车键。显示如图 12.3 所示。

```
管理员: 命令提示符
  TCP    [::]:445               [::]:0                 LISTENING
  TCP    [::]:2009              [::]:0                 LISTENING
  TCP    [::]:5357              [::]:0                 LISTENING
  TCP    [::]:49152             [::]:0                 LISTENING
  TCP    [::]:49153             [::]:0                 LISTENING
  TCP    [::]:49154             [::]:0                 LISTENING
  TCP    [::]:49155             [::]:0                 LISTENING
  TCP    [::]:49156             [::]:0                 LISTENING
  UDP    0.0.0.0:123            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:4500           *:*
  UDP    0.0.0.0:5355           *:*
  UDP    0.0.0.0:62856          *:*
  UDP    192.168.1.116:137      *:*
  UDP    192.168.1.116:138      *:*
  UDP    [::]:123               *:*
  UDP    [::]:500               *:*
  UDP    [::]:3702              *:*
  UDP    [::]:3702              *:*
  UDP    [::]:5355              *:*
  UDP    [::]:62857             *:*

C:\Users\Administrator>
```

图 12.3 “netstat –an”命令窗口

3. netstat –bn

所谓连接的宿主是指网络连接对应的应用程序或服务。通常情况下，仅凭开放端口是很难确认其安全与否的，发现可疑端口之后，首先要做的就是确认使用这些已经打开的端口的应用程序是哪个，然后进一步确认该程序是否为系统程序，如果不能确认，则可能是木马或其他非法程序。

在“管理员：命令提示符”窗口中，输入“netstat -bn”命令，按下回车键。显示如图 12.4 所示。

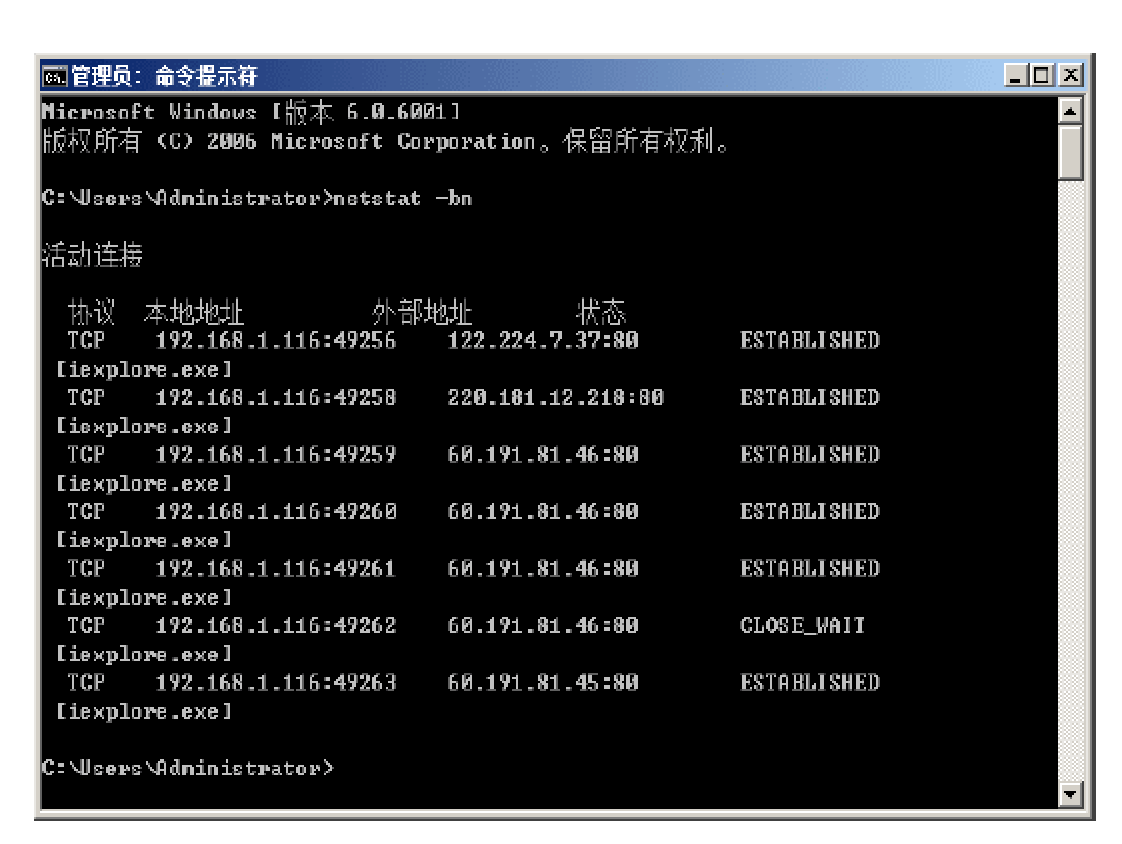


图 12.4 “netstat -bn”命令窗口

提示  CLOSE_WAIT 表示可以等待足够的时间以确保远程 TCP 接收到连接中断请求的确认。

在命令执行结果中，显示了当前活动的每个连接都是由哪些程序创建的，本例中端口 49256、49258、49259、49260、49261 以及 49263 都是由 iexplore.exe 程序打开的，均被用于访问外网的 Web 服务器，而 49262 是从本地用户发来的连接中断请求。如果在结果中发现计算机打开了可疑的端口，就可以使用该命令查看它调用了哪些组件，然后再检查各组件的创建时间和修改时间，如果发现异常，就可能是中了木马。

12.3.2　端口查询工具——PortQry

Portqry.exe 是 Windows Support Tools 中的一个实用命令行工具，其英文全称为 PortQry Command Line Port Scanner。PortQry 可以报告本地计算机或远程计算机上，目标 TCP 端口和用户数据报协议（UDP）端口的状态。Windows 2000/XP/2003 用户，可以从系统安装光盘中的支持工具包中获得，路径为：X:\SUPPORT\TOOLS\SUPPORT.CAB。Windows Vita/2008 用户则可以登录微软网站下载该工具，网址为：http://download.microsoft.com/download/0/d/9/0d9d81cf-4ef2-4aa5-8cea-95a935ee09c9/PortQryV2.exe。

1. PortQry 2.0 版的特性

PortQry 的最新版本为 2.0，相对于之前的 PortQry 1.22 而言，可以支持的通信协议更加丰富了，PortQry 2.0 可以准确地确定是否打开了比 PortQry 1.22 可以打开的 UDP 端口更多的端口。PortQry 2.0 支持以下会话层和应用层协议：

- 轻量目录访问协议（LDAP）。通过使用 TCP 和 UDP，PortQry 可以发送 LDAP 查询并正确解释 LDAP 服务器对该查询的响应。PortQry 对 LDAP 服务器的响应进行分析、格式设置，然后将其返回给用户；
- 远程过程调用（RPC）。通过使用 TCP 和 UDP，PortQry 可以发送 RPC 查询并正确解释对该查询的响应。该查询返回（转储）当前使用 RPC 终结点映射程序注册的所有终结点。PortQry 对 RPC 终结点映射程序的响应进行分析、格式设置，然后将其返回给用户；
- 域名系统（DNS）。通过使用 TCP 和 UDP，PortQry 可以发送格式正确的 DNS 查询，DNS 服务器是否返回否定响应并不重要，任何响应都指示该端口正在监听；
- NetBIOS 名称服务。默认情况下，NetBIOS 名称服务监听 UDP 端口 137。当 PortQry 确定此端口为监听还是筛选时，PortQry 执行相关操作以确定该端口是否确实正在监听。例如，如果正在运行 PortQry 的计算机上的 NetBIOS 可用，PortQry 会将 NetBIOS 适配器状态查询发送给目标计算机；如果目标计算机对此查询作出响应，PortQry 报告目标端口为监听，然后将目标计算机的 MAC 地址返回给用户；如果正在运行 PortQry 的计算机上的 NetBIOS 不可用，PortQry 不会尝试将 NetBIOS 适配器状态查询发送给目标计算机；
- 简单网络管理协议（SNMP）。SNMP 支持是 PortQry 2.0 中的新增特性。默认情况下，SNMP 服务监听 UDP 端口 161。为了确定端口 161 是否正在监听，PortQry 发送 SNMP 服务可以接受的格式的查询。SNMP 服务是使用社区名称或字符串配置的，必须知道该社区名称或字符串才能获取服务器的响应。使用 PortQry 可以在查询此端口时指定 SNMP 社区名称；
- Internet Security and Acceleration Server（ISA）。ISA Server 支持是 PortQry 2.0 中的新增功能。默认情况下，ISA Server 使用 TCP 端口 1745 和 UDP 端口 1745 与 Winsock 代理客户端和防火墙客户端通信。安装了 Winsock 代理客户端程序或防火墙客户端程序的计算机，使用这些端口从 ISA Server 请求服务和下载配置信息。为了确定端口是否正在监听，PortQry 发送 ISA Server 可以接受的格式的查询；

- SQL Server 2000 命名实例。SQL Server 2000 支持是 PortQry 2.0 中的新增功能。PortQry 查询 UDP 端口 1434 以查询正在 SQL Server 2000 计算机上运行的所有 SQL Server 命名实例。PortQry 发送 SQL Server 2000 可以接受的格式的查询，以确定此端口是否正在监听；
- 日常文件传输协议(TFTP)。TFTP 支持是 PortQry 2.0 中的新增功能。默认情况下，TFTP 服务器监听 UDP 端口 69。PortQry 发送 TFTP 服务器可以接受的格式的查询，以确定此端口是否正在监听；
- 第二层隧道协议（L2TP)。L2TP 支持是 PortQry 2.0 中的新增功能。路由选择和远程访问服务器以及其他 VPN 服务器监听 UDP 端口 1701，以进行入站 L2TP 连接。PortQry 发送 VPN 服务器可以接受的格式的查询，以确定此端口是否正在监听。

2. PortQry 概述

PortQry 的安装非常简单，下载或提取之后直接运行即可。安装完成后，打开命令提示符窗口，并转至 PortQry 的安装目录，即可执行各种查询命令。PortQry 提供如下三种查询模式，在不同的模式下，可以使用不同的命令行参数，实现相应的查询功能：

- 命令行查询模式：portqry -n name_to_query [-options]
- 交互模式：portqry -i [-n name_to_query] [-options]
- 本地模式：portqry -local | -wpid pid| -wport port [-options]

（1）命令行查询模式

简单查询模式下 PortQry 命令语法格式如下：

```
    portqry -n name to query [-p protocol] [-e | -r | -o endpoint(s)] [-q] [-l logfile]
[-sp source_port] [-sl] [-cn SNMP community name]
```

-n name_to_query——使用此参数指定目标计算机名称，此参数是必须的。可以指定主机名称或主机 IP 地址。但是，主机名称或 IP 地址中不能包括空格。PortQry 将主机名称解析为 IP 地址。如果 PortQry 无法将主机名称解析为 IP 地址，此工具会报告错误，并随后退出。如果输入 IP 地址，PortQry 将其解析为主机名称。如果解析不成功，PortQry 会报告错误，但仍继续处理命令。

该模式下的可选参数包括：

- -p protocol——指定用于连接目标计算机上目标端口的端口或协议的类型。如果不指定协议，PortQry 使用 TCP 作为协议。Protocol 的有效参数为 TCP、UDP 或 BOTH（即同时包含 TCP 和 UDP)。
- -e endpoint(s)——此参数用于指定目标计算机上的终结点（或端口号)。它必须是介于 1 和 65535（包括 1 和 65535）之间的有效端口号。不能将此参数与-o 或-r 参数一起使用。如果未指定端口号，PortQry 将查询端口 80。
- -o endpoint(s)——此参数用于指定按特定顺序查询的一定数量的端口。不能将此选项与-e 参数或-r 参数一起使用。使用此参数时，要使用逗号分隔端口号。可以按任意顺序输入端口号。但是，端口号和逗号分隔符之间不能留有空格。

- -r start port;end port——此参数用于指定要按先后顺序查询的端口号的范围。不能将此选项与-e 参数或-o 参数一起使用。使用此参数时，可以使用分号分隔起始端口号和终止端口号。指定的起始端口要小于终止端口。另外，端口号和分号之间不能有空格。使用此参数时，不查询 RPC 终结点映射程序。
- -q——使用此参数，可使 PortQry 取消除错误信息外的所有屏幕输出。在配置 PortQry 以便在批处理文件中使用时，此参数尤其有用。根据端口的状态，此参数的返回值也会有所不同。如果目标端口是监听，则返回 0；如果目标端口是未监听，则返回 1；如果目标端口为监听或筛选，则返回 2。

注意　只能将此参数与-e 参数一起使用。不能将此参数与-o 参数或-r 参数一起使用。此外，将-p 参数的值设置为 Both 时，也不能将此参数与-p 参数一起使用。将-q 参数与“-l logfile”参数一起使用时，PortQry 将覆盖具有相同名称的现有日志文件。

-l logfile——此参数用于指定记录 PortQry 生成的输出的日志文件。使用此参数时，请指定文件名和文件扩展名。不能在日志文件名中输入空格。在 PortQry 运行的文件夹中创建日志文件。PortQry 以文本格式生成日志文件输出。如果存在具有相同名称的现有日志文件，运行 PortQry 命令时系统将提示您覆盖此日志文件。

-sp source_port——使用此参数，可以指定连接到目标计算机上指定的 TCP 和 UDP 端口时要使用的初始源端口。此功能有助于测试筛选端口基于其源端口的防火墙或路由器规则。

-sl——使用此参数将导致 PortQry 等待 UDP 查询响应的时间更长。由于 UDP 无连接协议，所以 PortQry 无法确定端口是响应缓慢还是端口被筛选。在 PortQry 确定端口是未监听还是筛选之前，此选项使 PortQry 等待 UDP 端口响应的时间加倍。在速度较慢或不稳定的网络链接中查询 UDP 端口时，请使用此选项。

-cn SNMP community name——使用此参数，可以指定在发送 SNMP 查询时要使用的域名，但是必须用感叹号将域名字符串括起来。如果不对 SNMP 监听的某个端口进行查询，将忽略此参数。

（2）交互模式

使用 PortQry 1.22 版，用户可以从命令提示窗口的命令行对端口进行查询。当解决计算机间的连接问题时，可能需要输入许多重复的命令。在 PortQry 2.0 中，用户可以用此方式运行命令，但是 PortQry 2.0 版还具有交互模式。该交互模式类似于 Nslookup DNS 实用工具或 Nblookup WINS 实用工具的交互功能。

交互模式下 PortQry 命令语法格式如下：

```
portqry -i [-n name_to_query] [-options]
```

-i 参数的主要作用就是进入交互模式下，是必须的。该模式下的可用参数包括：

phelp 或?p——显示本地主机经常使用的端口。

node NAME——显示默认主机的 IP 地址或计算机名。

query 或 q——向默认主机发送查询命令。

set OPTION=value——重新设置要查询的目标参数，包括端口号、协议等。其中，OPTION

代表如下参数：

all——显示当前默认设置。

port=n——设置要查询的端口号。

sport=n——设置源端口号。

protocol=p——设置查询端口的通信协议类型，TCP、UDP 或者两者均包括。

cn=string——指定在发送 SNMP 查询时要使用的社区字符串或社区名称。

nr——使用反向名称查询，此时 PortQry 不查询返回主机名的 IP 地址，PortQry 立即查询目标端口。

sl——使用慢速连接，延长 UDP 查询的返回时间。

（3）本地模式

PortQry 的本地模式操作旨在提供有关运行 PortQry 的本地计算机上的 TCP 端口和 UDP 端口的详细信息。该模式下 PortQry 命令语法格式如下：

```
portqry -local | -wpid pid | -wport port [-wt seconds] [-l logfile] [-v]
```

注意 

-local、-wpid pid 和-wport port 是 PortQry 的本地模式提供的三种基本命令，只能任选其一，但该参数是必需的。

各参数的具体功能如下：

-local——尝试枚举本地计算机上当前所有活动的 TCP 和 UDP 端口映射。该输出与 netstat.exe -an 命令生成的输出类似。

-wpid pid——监视指定的进程 ID（PID）是否发生变化。这些变化可能包括到端口的连接数的增减或任一现有连接的连接状态的变化。此命令支持的可选参数与监视端口命令支持的相同。

-wport port——监视某个指定端口是否发生变化。这些变化可能包括到端口的连接数的增减或任一现有连接的连接状态的变化。

-wport port 命令下还包括如下可选参数，这些可选参数不可应用于另外两种命令提示符下：

-v——获取指定端口的其他状态信息。

-wt——配置 PortQry 自动检查指定端口状态变化的时间间隔，可选范围为 1~1 200 秒。系统默认为 60 秒。

-l——记录监视端口命令的输出结果。

（4）返回端口状态的方式

Portqry.exe 通过以下 3 种不同方式报告系统端口的状态：

- 监听。某些进程正在监听所选计算机系统的端口，Portqry.exe 收到该端口的响应。
- 未监听。没有进程监听目标系统上的目标端口。Portqry.exe 收到目标 UDP 端口发回的“Destination Unreachable-Port Unreachable”（无法达到目标-无法达到端口）消息。或者，如果目标端口是 TCP 端口，Portqry 则收到已设置重置标志的 TCP 确认数据包。

■ 筛选。目标计算机系统的端口正在被筛选。Portqry.exe 没有收到该端口的响应。进程可能在监听端口，也可能不在监听端口。默认情况下，在报告目标端口被筛选之前，将对 TCP 端口查询三次，对 UDP 端口查询一次。Portqry.exe 可查询单个端口、端口的顺序列表或多个连续的端口。

3. PortQry 命令行模式实例

（1）LDAP 查询并正确解释 LDAP 服务器对该查询的响应

在命令提示符下，输入如下命令：

```
portqry -n coolpen.net -p udp -e 389
```

按 Enter 键执行命令，显示如图 12.5 所示结果。

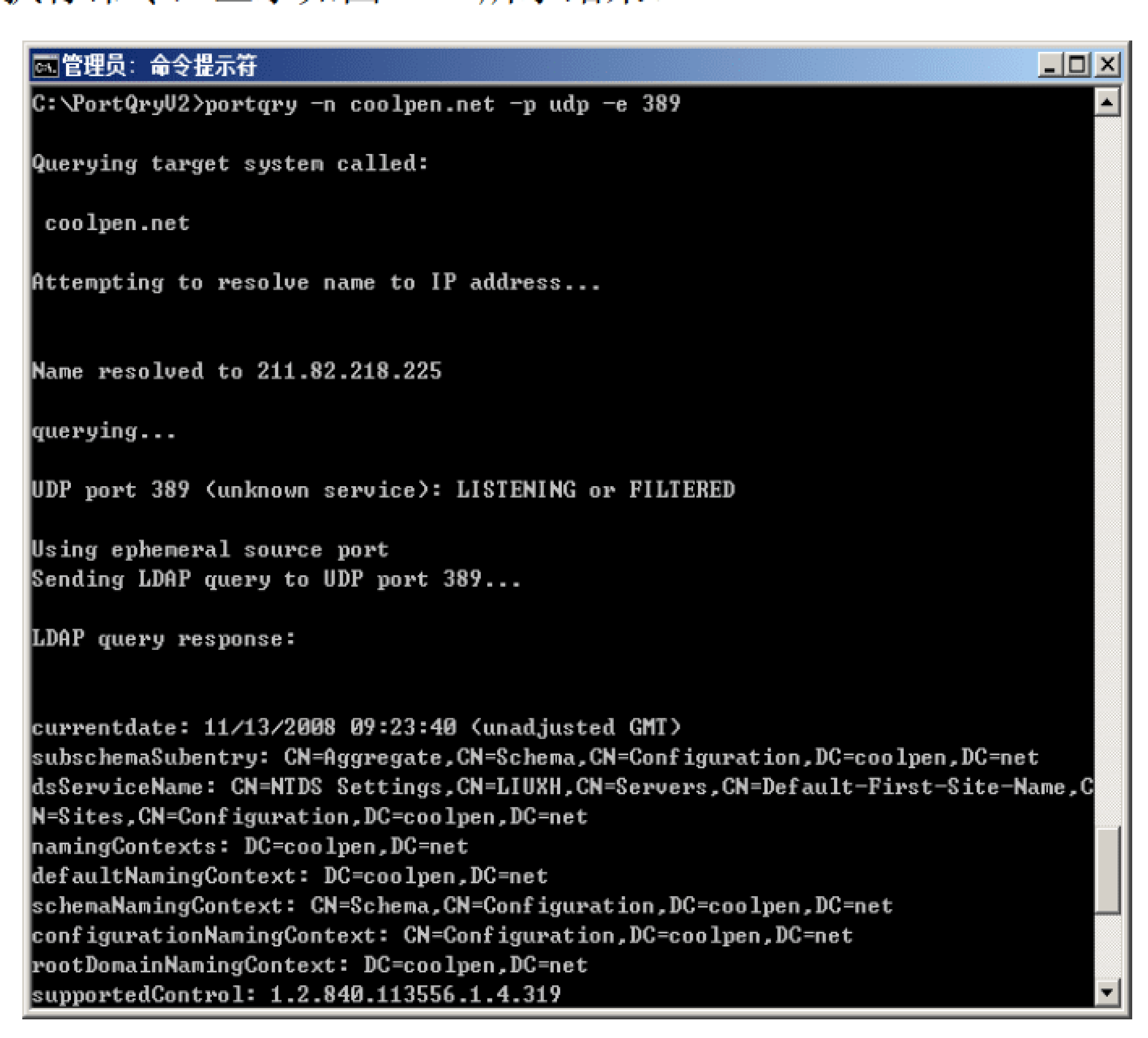


图 12.5　LDAP 查询并正确解释 LDAP 服务器对该查询的响应

通过使用 TCP 和 UDP，PortQry 可以发送 LDAP 查询并正确解释 LDAP 服务器对该查询的响应。PortQry 对 LDAP 服务器的响应进行分析、格式设置，然后将其返回给用户。

执行过程如下：

PortQry 使用“%SYSTEMROOT%\system32\drivers\Etc”文件夹中的 Services 文件解析 UDP 端口 389。如果 PortQry 将该端口解析为 LDAP 服务，PortQry 会将无格式的用户数据包发送到目标计算机上的 UDP 端口 389。如果 PortQry 没有收到目标端口的响应，原因是 LDAP 服务只响应格式正确的 LDAP 查询。

使用该命令，PortQry 将报告端口是监听或筛选。PortQry 将格式正确的 LDAP 查询发送给目标计算机上的 UDP 端口 389。如果 PortQry 收到对此查询的响应，它会将整个查询返回给用户，并报告端口是监听。如果 PortQry 没有收到对此查询的响应，将报告该端口是筛选。

（2）发送 RPC 查询并正确解释对该查询的响应

在命令提示符下，输入如下命令：

```
portqry -n coolpen.net -p udp -e 135
```

按 Enter 键执行命令，运行后的结果显示如图 12.6 所示。

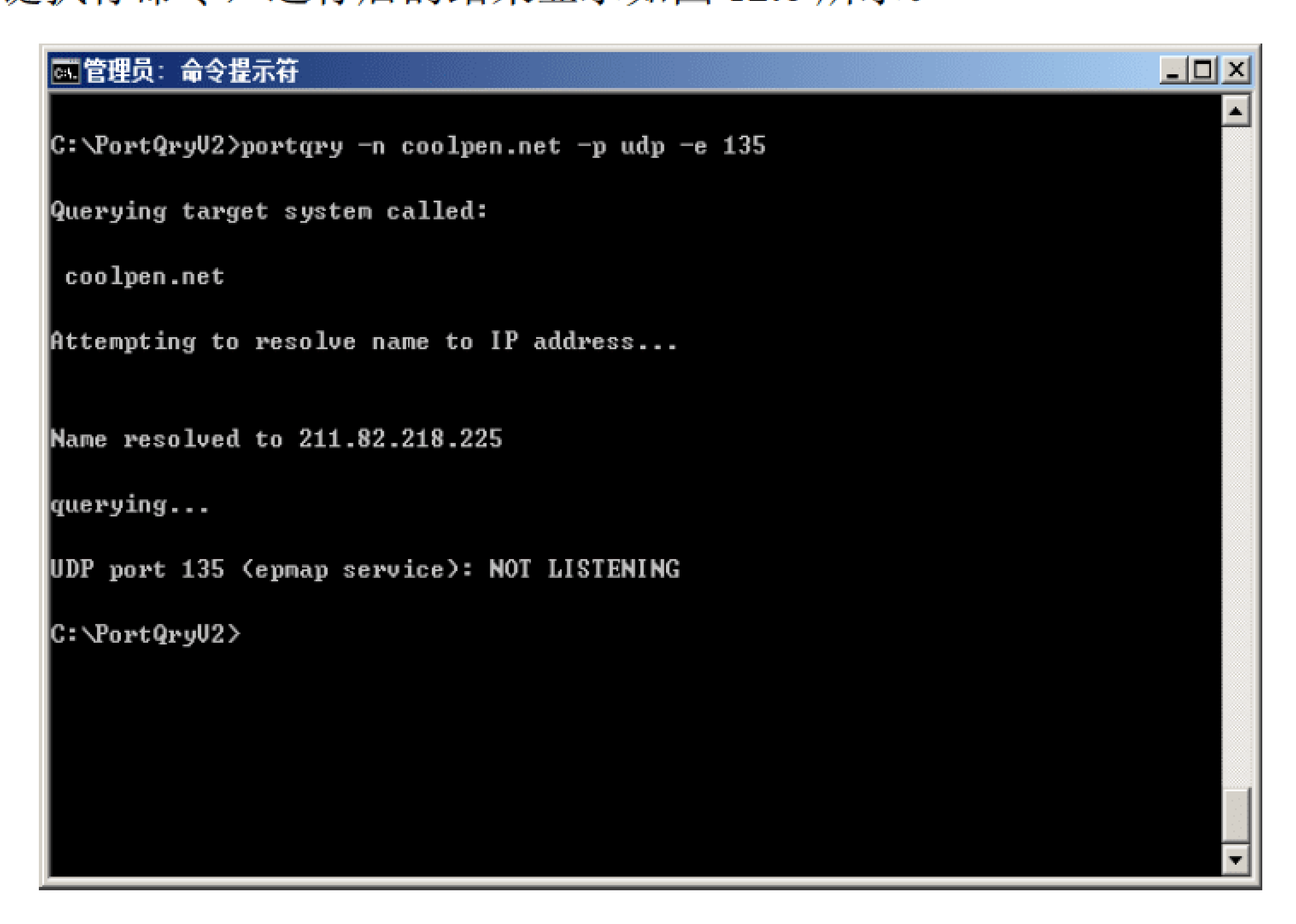


图 12.6　发送 RPC 查询并正确解释对该查询的响应

通过使用 TCP 和 UDP，PortQry 可以发送 RPC 查询并正确解释对该查询的响应。该查询返回（转储）当前使用 RPC 终结点映射程序注册的所有终结点。PortQry 对 RPC 终结点映射程序的响应进行分析、格式设置，然后将其返回给用户。

PortQry 执行以下操作：

PortQry 使用“%SYSTEMROOT%\System32\Drivers\Etc”文件夹中的 Services 文件解析 UDP 端口 135。如果 PortQry 将该端口解析为 RPC 终结点映射程序服务（Epmap），PortQry 会将无格式的用户数据包发送给目标计算机上的 UDP 端口 135。如果 PortQry 没有收到目标端口的响应，原因可能是 RPC 终结点映射程序服务，只响应格式正确的 RPC 查询。

使用该命令，PortQry 将报告端口是监听或筛选。PortQry 将格式正确的 RPC 查询发送给目标计算机上的 UDP 端口 135，并返回当前使用 RPC 终结点映射程序注册的所有终结点。如果 PortQry 收到对此查询的响应，PortQry 会将整个响应返回给用户并报告该端口为监听。如果 PortQry 没有收到对此查询的响应，则将报告端口筛选。

（3）NetBIOS 名称服务监听 UDP 端口 137

在命令提示符下，输入如下命令：

portqry –n coolpen.net –p udp –e 137

按 Enter 键执行命令，运行后的结果显示如图 12.7 所示。默认情况下，NetBIOS 名称服务监听 UDP 端口 137。

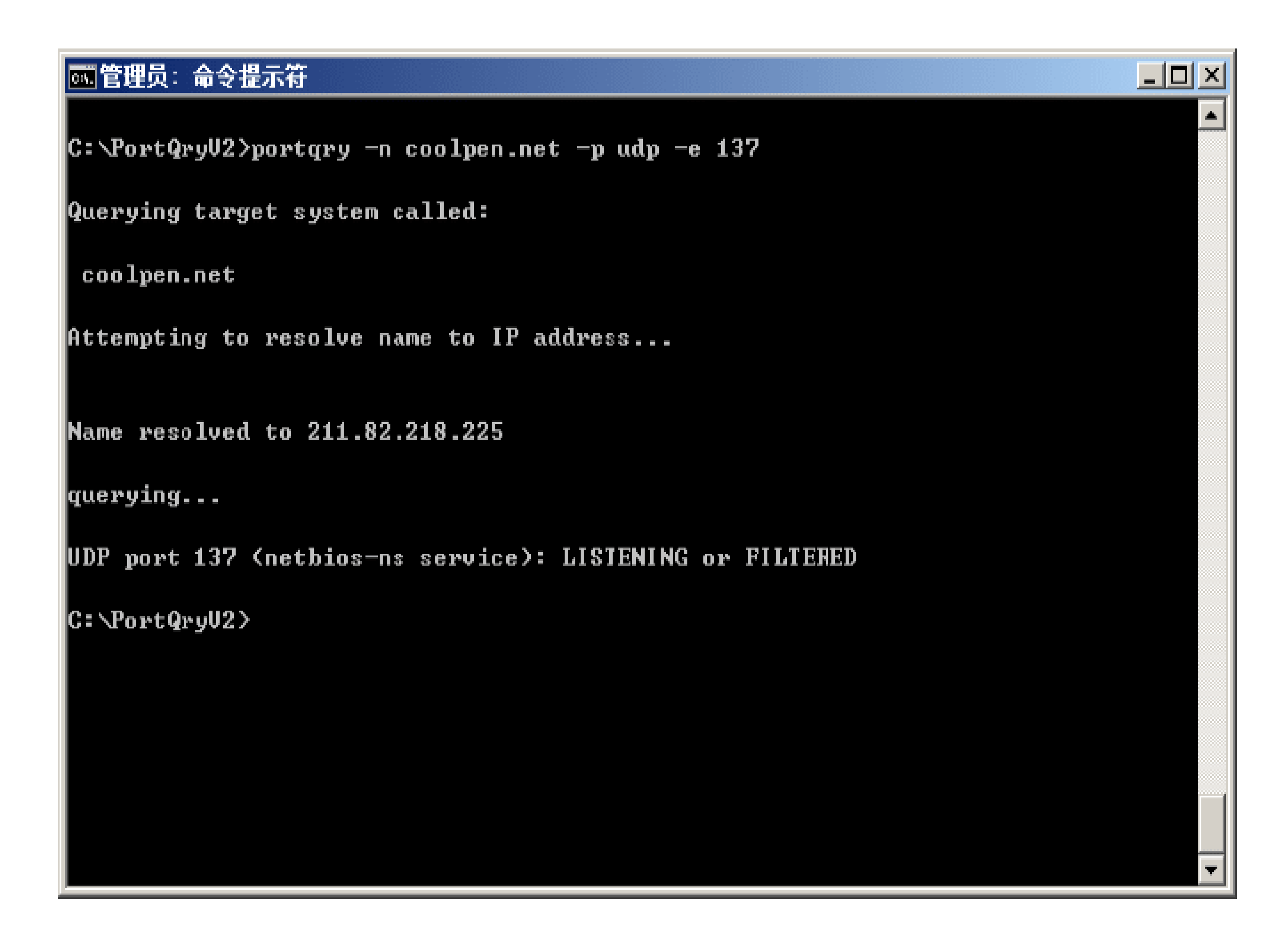


图 12.7　查看 NetBIOS 名称服务监听 UDP 端口 137

（4）查看远程主机的 445 端口

借助 Portqry 命令，还可以查看远程主机的某个端口工作状态，此时需要使用“Portqry –n”模式。例如，在命令提示符窗口中，转至 Portqry 所在目录下，输入如下命令：

```
Portqry -n hstjl-pc -e 445
```

按 Enter 键执行命令，显示如图 12.8 所示运行结果。

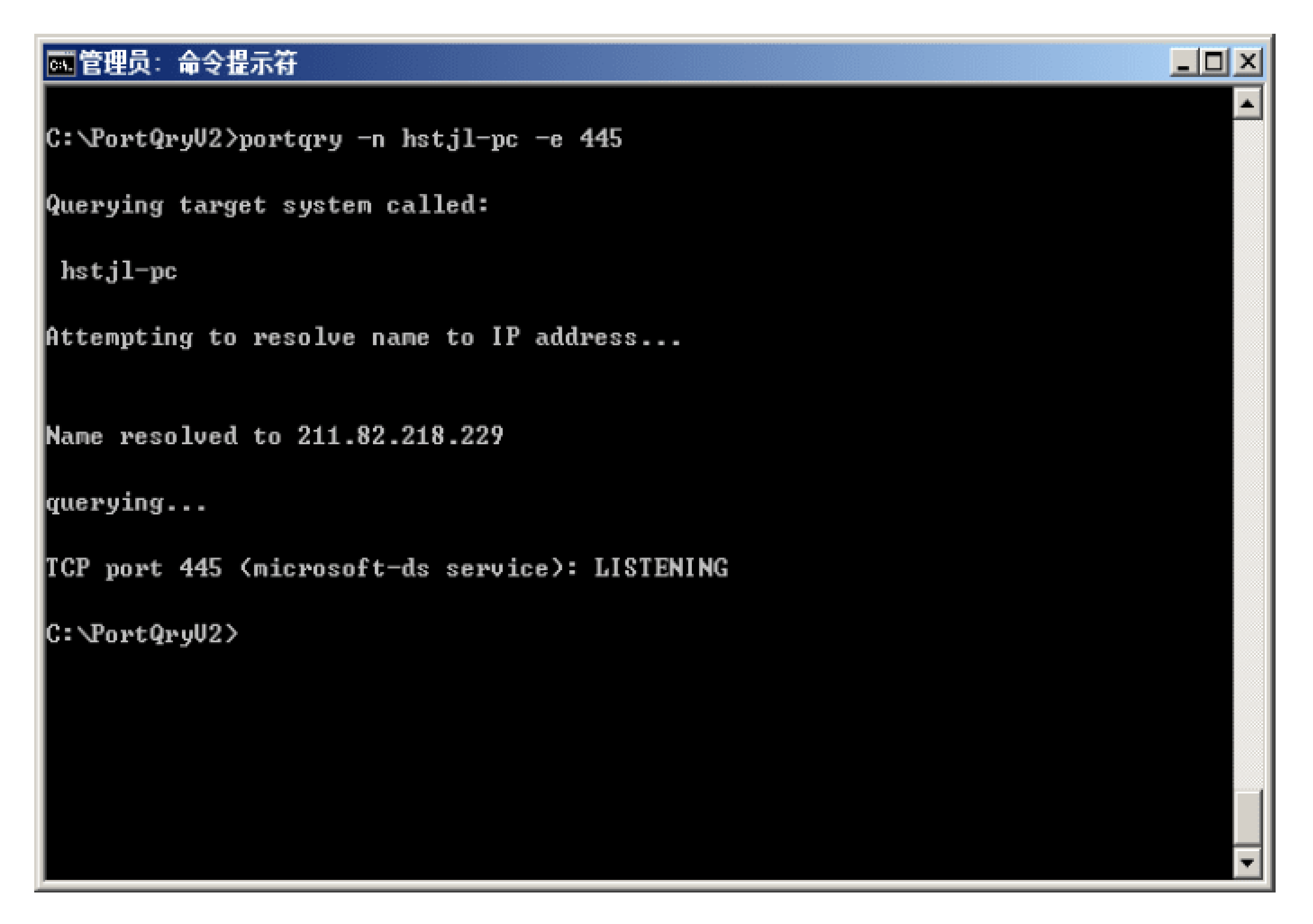


图 12.8　查看远程主机端口状态

运行结果显示目标计算机系统的 445 端口，目前正处于 LISTENING（监听）状态。

（5）查询多个指定端口并输出到日志

在命令提示符下，输入如下命令：

```
portqry -n 211.82.218.229 -p tcp -o 143,110,25 -l portqry.log
```

按 Enter 键执行命令，显示如图 12.9 所示运行结果。

```
管理员: 命令提示符
C:\PortQryV2>portqry -n 211.82.218.229 -p tcp -o 143,110,25 -l portqry.log
Creating log file called portqry.log
Querying target system called:
 211.82.218.229
Attempting to resolve IP address to a name...

IP address resolved to hstjl-PC
querying...
TCP port 143 (imap service): FILTERED
TCP port 110 (pop3 service): FILTERED
TCP port 25 (smtp service): FILTERED
Log file portqry.log successfully created in current directory
C:\PortQryV2>
```

图 12.9　查询多个端口状态

首先，portqry 命令会尝试将指定 IP 地址解析为主机名，然后查询所指定的主机上的 TCP 端口 143、110 和 25（按该顺序查询），最后，该命令还会创建一个日志文件（文件名为 Portqry.log），并将所有运行结果输出的日志。用户也可以在资源管理器中，打开该日志，如图 12.10 所示。

如果需要查询的端口数量较多，且彼此连续，则可以通过直接指定端口号段的方式，查询多个连续端口状态。例如，在命令提示符下，输入如下命令：

```
portqry -n coolpen.net -r 135:139
```

按 Enter 键执行命令，显示如图 12.11 所示结果。

在此过程中，portqry 会依次对端口 135~139 进行扫描，并返回其状态信息。

```
portqry - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
PortQry Version 2.0 Log File
System Date: Thu Nov 13 18:09:27 2008
Command run:
 portqry -n 211.82.218.229 -p tcp -o 143,110,25 -l portqry.log
Local computer name:
 LIUXH
Querying target system called:
 211.82.218.229
Attempting to resolve IP address to a name...

IP address resolved to hstjl-PC
querying...
TCP port 143 (imap service): FILTERED
TCP port 110 (pop3 service): FILTERED
TCP port 25 (smtp service): FILTERED
```

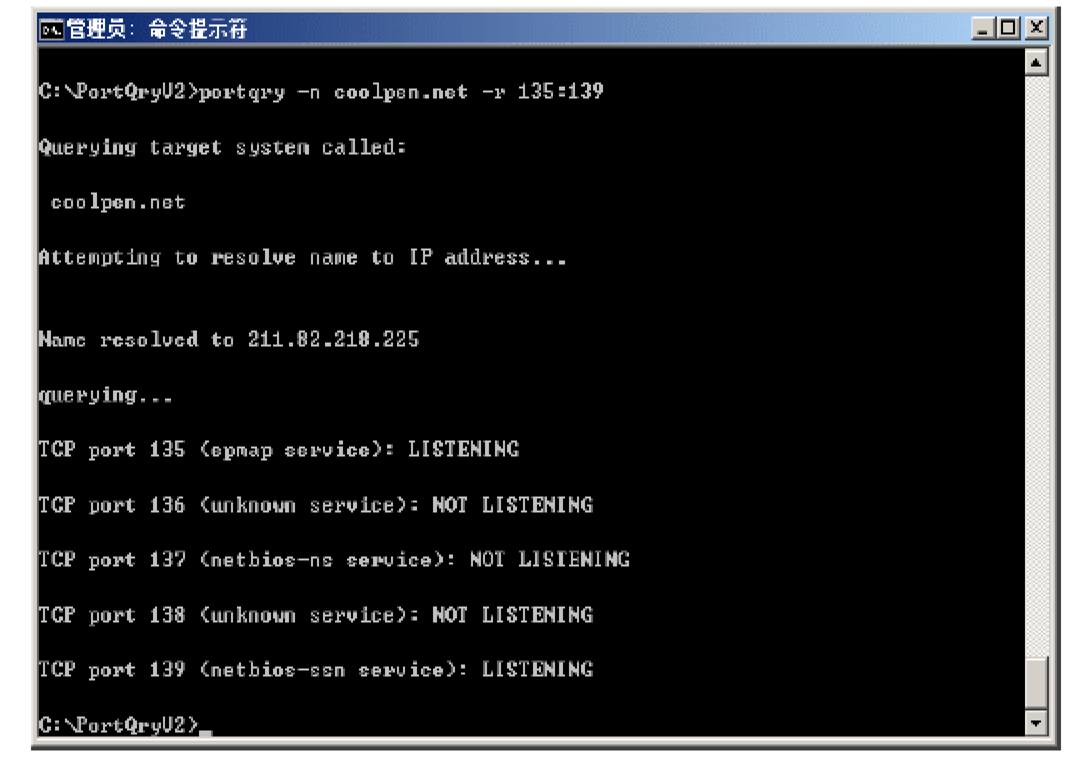


图 12.10　查看输出的日志文件　　　　图 12.11　扫描端口号段

（6）借助域名实现 SNMP 查询

通过 SNMP 查询管理员可以确定目标计算机的 SNMP 服务使用的端口，是否处于监听状态。默认情况下，SNMP 服务监听 UDP 端口 161。在命令提示符下，输入如下命令：

```
portqry -n www.coolpen.org -p udp -e 161 -cn !coolpen!
```

按 Enter 键执行命令，显示如图 12.12 所示结果。本次查询过程中使用的 SNMP 字符串为 coolpen。

```
C:\PortQryV2>portqry -n www.coolpen.org -p udp -e 161 -cn !coolpen!
Querying target system called:
 www.coolpen.org
Attempting to resolve name to IP address...

Name resolved to 121.17.46.82
querying...
UDP port 161 (snmp service): LISTENING or FILTERED
community name for query:
 coolpen
Sending SNMP query to UDP port 161...
UDP port 161 (snmp service): FILTERED
C:\PortQryV2>
```

图 12.12　查询 SNMP 端口的监听状态

（7）编译 PortQry 批处理文件

当需要查询的端口数量较多时，需要等待的时间会比较长，返回的结果信息也会非常多，而命令提示符窗口的信息容量是有限的，即信息量过大时，无法显示较早的信息。此时，用户可以在安静模式下，执行对指定端口的状态查询，只需编译一个 Portqry 批处理文件即可。新建一个空白记事本文件，输入如下信息，并保存为.bat 文件：

```
:Top
portqry -n 127.0.0.1 -e 135 -p tcp -q -l bendi135.txt
if errorlevel = 2 goto filtered
if errorlevel = 1 goto failed
if errorlevel = 0 goto success
goto end

:filtered
Echo Port is listening or filtered
goto end

:failed
Echo Port is not listening
Goto end

:success
Echo Port is listening
goto end
:end
```

```
PortQry Version 2.0 Log File
System Date: Fri Nov 14 10:41:55 2008
Command run:
 portqry -n 127.0.0.1 -e 135 -p tcp -q -l bendi135.txt
Local computer name:
 LIUXH
Querying target system called:
 127.0.0.1
Attempting to resolve IP address to a name...

IP address resolved to liuxh.coolpen.net
querying...
TCP port 135 (epmap service): LISTENING

======== end of log file ========
  PortQry developed by Tim Rains
```

图 12.13　执行结果

需要执行查询时，用户无需打开命令提示符窗口，只需在资源管理器中双击创建的批处理文件，即可开始执行文件中指定的查询命令。查询过程中，用户无需任何操作，窗口中也不会显示任何过程信息，可以直接将执行窗口最小化。完成后，portqry 会自动将结果信息保存到指定的日志文件中。打开该文件，即可查看详细执行过程，如图 12.13 所示。

4. PortQry 交互模式实例

（1）进入 PortQry 交互模式

交互模式是 PortQry 的新增功能之一，也是 PortQry 的一个特殊子环境，主要用于设置 PortQry 命令的相关参数，例如，是否自动解析名称、默认 SNMP 字符串值等。在命令提示符下，转入 PortQry 命令所在目录，输入如下命令：

```
Portqry-i
```

按 Enter 键执行命令，即可进入交互模式，显示如图 12.14 所示结果。用户可以使用“?”或“help”命令，查看该模式下可以使用的命令及选项。

```
管理员: 命令提示符 - portqry -i
C:\PortQryV2>portqry -i

PortQry Interactive Mode

Type 'help' for a list of commands

Default Node: 127.0.0.1

Current option values:
   end port=    80
   protocol=    TCP
   source port= 0 (ephemeral)
> help

Valid Commands:
===============

help or ?        - display info on common commands
phelp or ?p      - display list of frequently used ports

node NAME        - set default node to query, NAME or IP address

query or q       - send query to default node

set OPTION=value

Options:
    all          - display current option values
```

图 12.14　进入交互模式

注意　使用 exit 或 quit 命令均可退出 PortQry 交互模式。

（2）查看当前 PortQry 命令的默认设置

在 PortQry 交互模式下输入如下命令：

```
set all
```

按 Enter 键执行命令，显示如图 12.15 所示结果。

```
管理员: 命令提示符 - portqry -i

C:\PortQryV2>portqry -i

PortQry Interactive Mode

Type 'help' for a list of commands

Default Node: 127.0.0.1

Current option values:
   end port=    80
   protocol=    TCP
   source port= 0 (ephemeral)
> set all

Default Node: 127.0.0.1

Current option values:
   end port=    80
   protocol=    TCP
   source port= 0 (ephemeral)
   Reverse name lookup enabled
   SNMP community name: public

> _
```

图 12.15　查看 PortQry 命令的默认设置

从结果中可以看出，PortQry 命令默认查询的主机为 127.0.0.1，即本地计算机；默认查询的端口协议为 TCP；默认查询的端口为 80；自动执行解析功能，即如果输入主机名或域名，执行命令时先解析为 IP 地址，反之亦然；默认的 SNMP 字符串值为 public。

（3）更改默认查询主机和端口协议

在 PortQry 交互模式下，可以修改 PortQry 的各项默认参数。例如，在交互模式下，分别输入如下命令：

```
node 211.82.218.229
set protocol=both
```

按 Enter 键执行命令，修改默认参数。为验证命令效果，可以使用 set all 命令查看，如图 12.16 所示。

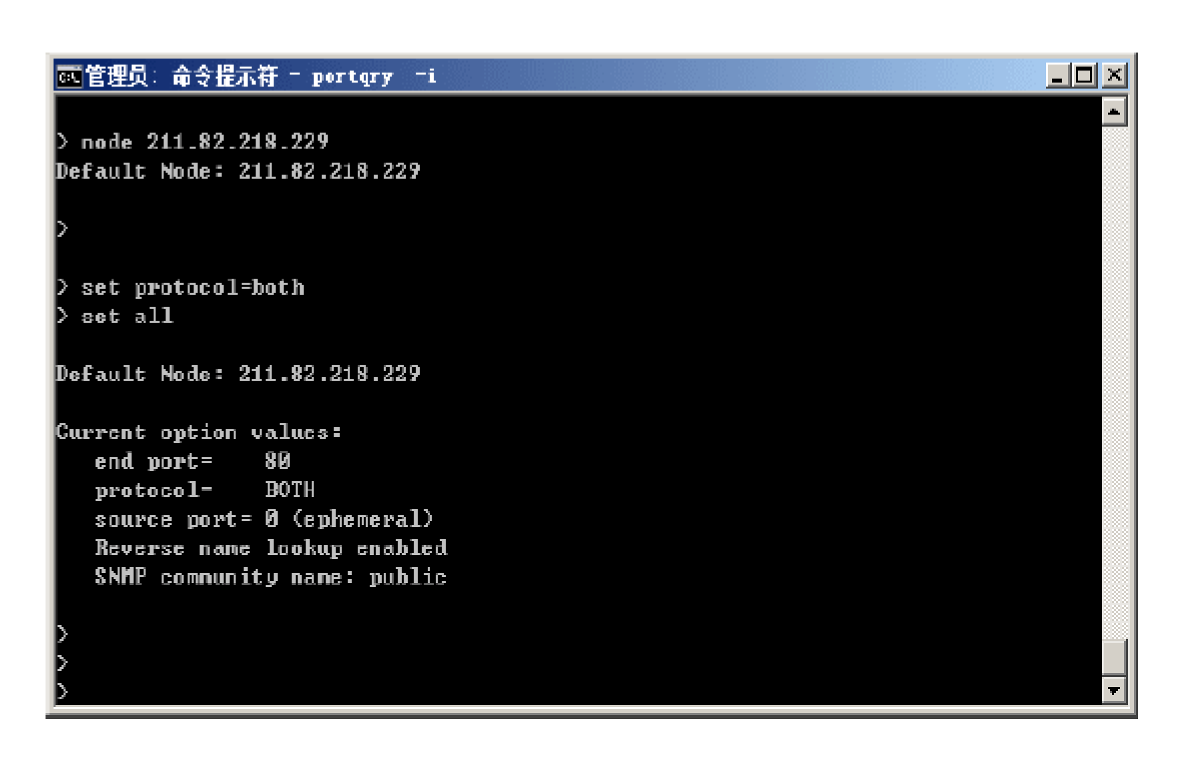


图 12.16　修改默认查询主机和端口协议

（4）快速查询 DNS 服务对应端口状态

在交互模式下，除可以修改 Portqry 命令的各项参数之外，还可以执行多种常规端口的快速查询，如 FTP 服务对应的 21、20 端口，DNS 服务使用的 53 端口等。在交互模式下，输入如下命令：

```
q dns
```

按 Enter 键执行命令，显示如图 12.17 所示结果。需要注意的是，此时都是按照 Portqry 命令的默认设置执行命令的，即目标计算机为默认主机。

```
管理员: 命令提示符 - portqry -i
> q dns

resolving service name using local services file...
UDP port resolved to the 'domain' service

IP address resolved to liuxh.coolpen.net

querying...

UDP port 53 (domain service): LISTENING

>

resolving service name using local services file...
TCP port resolved to the 'domain' service

IP address resolved to liuxh.coolpen.net

querying...

TCP port 53 (domain service): LISTENING

>
```

图 12.17　快速查询端口状态

5. PortQry 本地模式实例

（1）查询本地所有活动端口

查看本地计算机端口状态及开放情况，应使用“portqry”命令的 local 工作模式。打开命令提示符窗口，转至 Portqry 所在目录下，输入如下命令：

```
portqry -local
```

按 Enter 键执行命令，显示如图 12.18 所示结果。

```
管理员: 命令提示符
C:\PortQryV2>portqry -local


Processing local system's ports...

Port to process mappings unavailable

TCP/UDP Port Usage

45 active ports found

Port          Local IP          State          Remote IP:Port
TCP 53        127.0.0.1         LISTENING      0.0.0.0:0
TCP 53        211.82.218.225    LISTENING      0.0.0.0:0
UDP 53        127.0.0.1                        *:*
UDP 53        211.82.218.225                   *:*
TCP 80        0.0.0.0           LISTENING      0.0.0.0:0
TCP 80        211.82.218.225    ESTABLISHED    211.82.218.229:51407
TCP 88        0.0.0.0           LISTENING      0.0.0.0:0
UDP 88        211.82.218.225                   *:*
UDP 123       0.0.0.0                          *:*
TCP 135       0.0.0.0           LISTENING      0.0.0.0:0
UDP 137       211.82.218.225                   *:*
UDP 138       211.82.218.225                   *:*
TCP 139       211.82.218.225    LISTENING      0.0.0.0:0
TCP 389       0.0.0.0           LISTENING      0.0.0.0:0
UDP 389       211.82.218.225                   *:*
```

图 12.18　本地计算机端口开放情况

执行结果中，显示目前本地主机上处于活动状态的端口数量，及详细连接信息，包括端口号、本地 IP 地址、状态、远程计算机的 IP 地址和端口号等。

（2）查询本地指定端口状态

监听本地系统端口状态操作，在 Windows Vista 和 Windows Server 2008 系统中是无法实现的，该命令只能应用于 Windows 2000/XP/2003 系统。在命令提示符窗口中，输入如下命令：

```
portqry -wport 139
```

按 Enter 键执行命令，显示如图 12.19 所示结果。

```
命令提示符 - portqry -wport 139
C:\PortQryV2>portqry -wport 139

PortQry Version 2.0
Watching port: 139

Checking for changes every 60 seconds

**press escape to stop watching port

============
System Date: Fri Nov 14 14:44:20 2008


PID     Port          Local IP          State          Remote IP:Port
4       TCP 445       0.0.0.0           LISTENING      0.0.0.0:34908
4       TCP 139       211.82.218.241    LISTENING      0.0.0.0:12530
4       TCP 1031      211.82.218.241    ESTABLISHED    211.82.218.229:445
4       UDP 445       0.0.0.0                          *:*
4       UDP 137       211.82.218.241                   *:*
4       UDP 138       211.82.218.241                   *:*

Port Statistics

TCP mappings: 3
UDP mappings: 3

TCP ports in a LISTENING state:        2 = 66.67%
TCP ports in a ESTABLISHED state:      1 - 33.33%
```

图 12.19　监听本地计算机的 139 端口

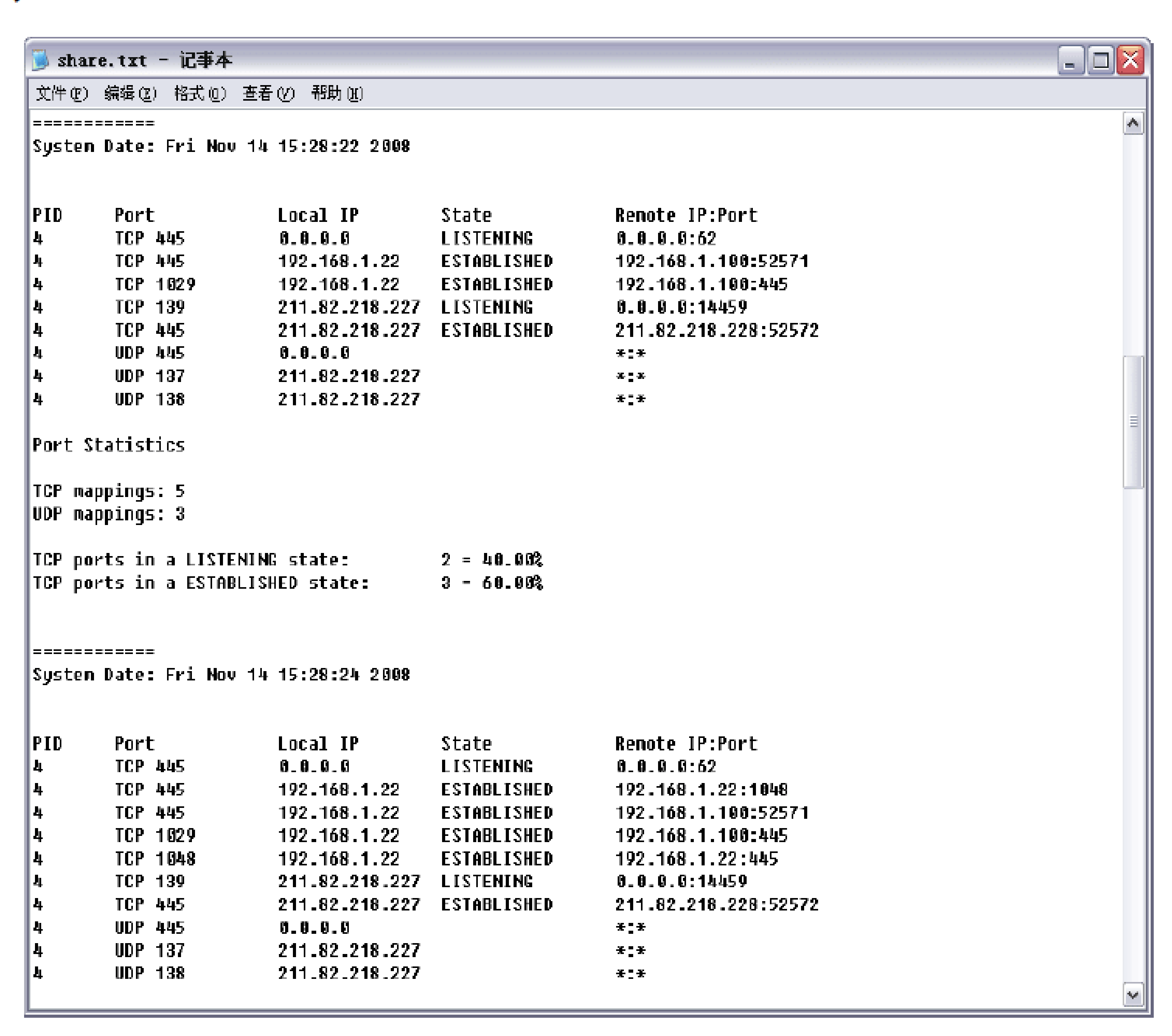
默认情况下，执行上述命令后，portqry 将持续监听 139 端口的工作情况，并且每 60 秒钟刷新一次结果，直至用户按下“ESC”键，结束监听为止。在此过程中，监听结果将随着端口状态的变化而自动记录。

（3）每隔 2 秒钟查询一次 445 端口的状态

在命令提示符下，输入如下命令：

```
portqry -wport 445 -wt 2 -l share.txt
```

按 Enter 键执行命令，即可开始将监视结果输出到日志文件中，并且每隔 2 秒钟，自动刷新一次。需要停止时，按下 ESC 键即可。在资源管理器中，打开日志文件即可查看详细信息，如图 12.20 所示。




```
============
System Date: Fri Nov 14 15:28:22 2008


PID     Port            Local IP        State           Remote IP:Port
4       TCP 445         0.0.0.0         LISTENING       0.0.0.0:62
4       TCP 445         192.168.1.22    ESTABLISHED     192.168.1.100:52571
4       TCP 1029        192.168.1.22    ESTABLISHED     192.168.1.100:445
4       TCP 139         211.82.218.227  LISTENING       0.0.0.0:14459
4       TCP 445         211.82.218.227  ESTABLISHED     211.82.218.228:52572
4       UDP 445         0.0.0.0                         *:*
4       UDP 137         211.82.218.227                  *:*
4       UDP 138         211.82.218.227                  *:*

Port Statistics

TCP mappings: 5
UDP mappings: 3

TCP ports in a LISTENING state:         2 = 40.00%
TCP ports in a ESTABLISHED state:       3 - 60.00%


============
System Date: Fri Nov 14 15:28:24 2008


PID     Port            Local IP        State           Remote IP:Port
4       TCP 445         0.0.0.0         LISTENING       0.0.0.0:62
4       TCP 445         192.168.1.22    ESTABLISHED     192.168.1.22:1048
4       TCP 445         192.168.1.22    ESTABLISHED     192.168.1.100:52571
4       TCP 1029        192.168.1.22    ESTABLISHED     192.168.1.100:445
4       TCP 1048        192.168.1.22    ESTABLISHED     192.168.1.22:445
4       TCP 139         211.82.218.227  LISTENING       0.0.0.0:14459
4       TCP 445         211.82.218.227  ESTABLISHED     211.82.218.228:52572
4       UDP 445         0.0.0.0                         *:*
4       UDP 137         211.82.218.227                  *:*
4       UDP 138         211.82.218.227                  *:*
```

图 12.20　每隔 2 秒钟查询一次 445 端口的状态

（4）监视指定的进程 ID（PID）变化情况

在命令提示符下输入如下命令：

```
portqry -wpid 468 -wt 30 -l pid.txt
```

按 Enter 键执行命令。停止监视后，打开日志文件，显示如图 12.21 所示结果。

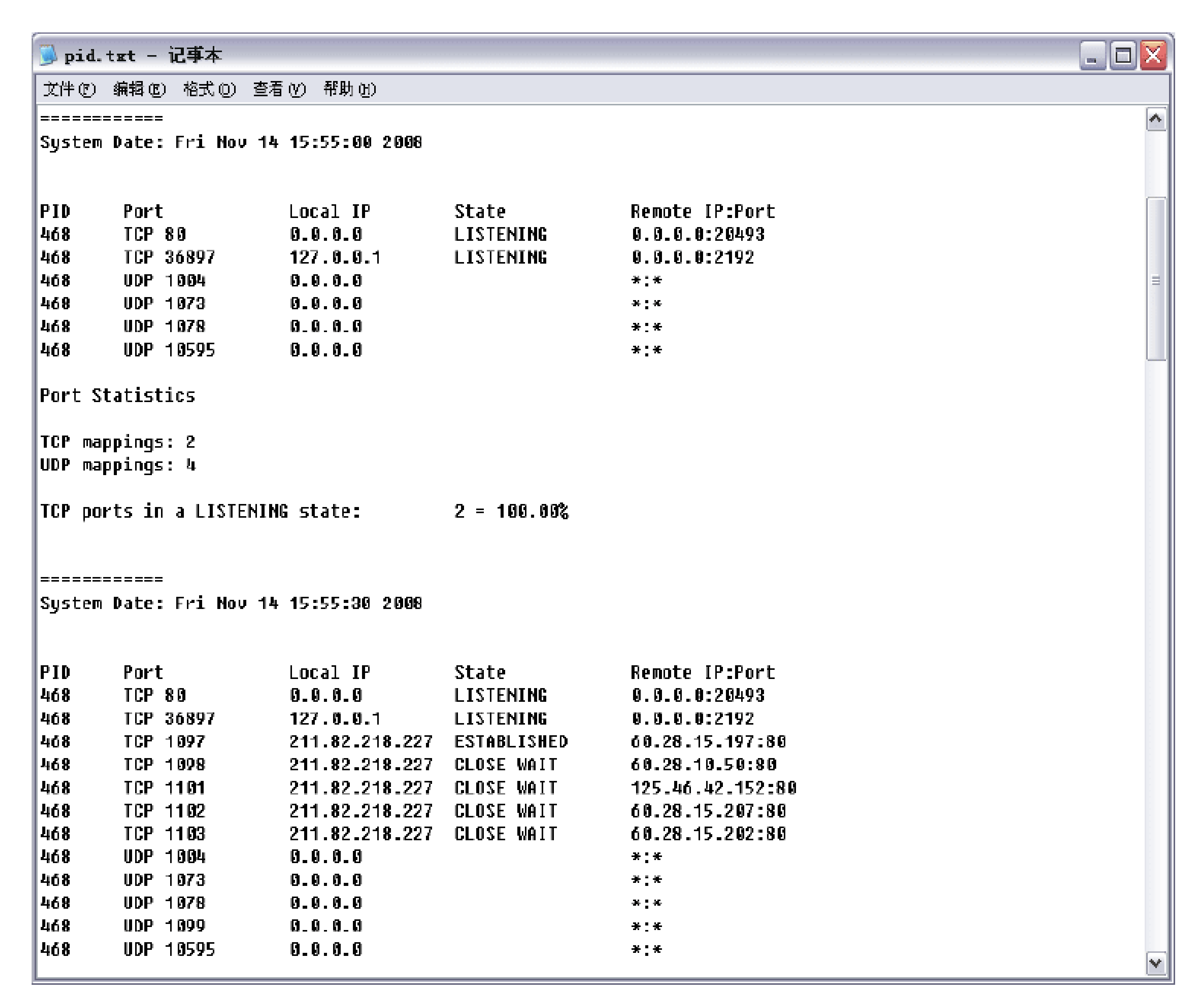


图 12.21　显示监视 PID 进程的变化

利用监视 PID 命令，PortQry 可以监视指定的进程 ID（PID）是否发生变化，这些变化包括到端口的连接数的增减或任一现有连接的连接状态的变化。此命令支持的可选参数与监视端口命令支持的相同。

12.3.3　借助第三方软件查看端口

与 netstat 命令类似，端口监视类软件也能查看本机打开了哪些端口，这类软件非常多，如果上网，以 TCPView 软件为例，密切监视本机端口连接情况，既能严防非法连接，也能确保网络安全。

TCPView 是一个查看端口和线程的小工具，只要木马在内存中运行，便会打开某个端口；只要黑客进入主机，就会有新的线程。

01 下载、安装并运行 TCPView 软件。打开 TCPView 窗口，依次选择“选项”→“字体”命令，设置字体大小，解决默认字体太小而无法看清的问题，显示如图 12.22 所示窗口。

02 在 TCPView 窗口中，可以很容易看出某个端口是什么程序打开的。用户可以通过图标类型来分别哪些是正常的应用程序打开的端口。对于系统本身打开的端口，由于一般用户并不太熟悉，可以通过检查线程的属性来判断。右击某个进程，在弹出的快捷菜单中选择“进程属性”命令，显示如图 12.23 所示“属性”对话框。

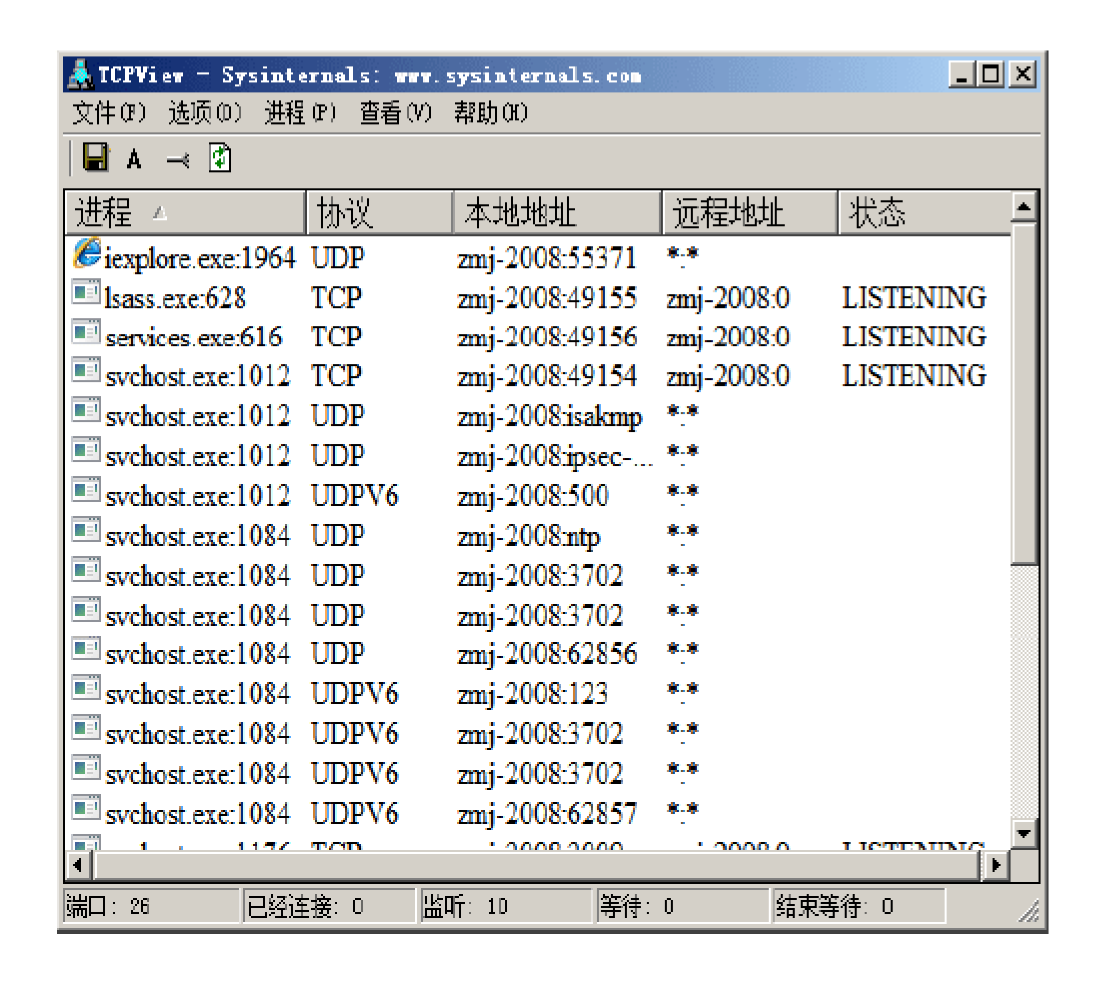


图 12.22　TCPView 窗口

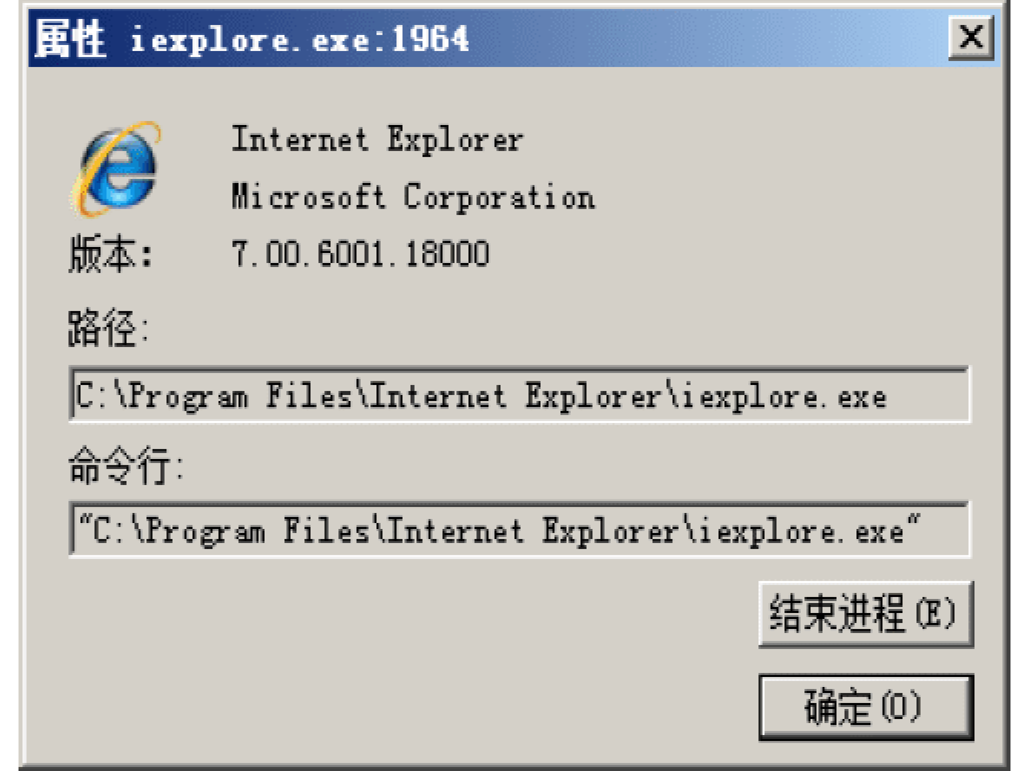


图 12.23　“属性”对话框



提示　如果出现和系统程序相似的名字，文件又不在系统目录，那么这些程序就有可能是假冒的系统程序，极有可能是木马。

12.3.4　借助第三方软件扫描端口

通常情况下，绝对禁止在服务器上运行来历不明的应用程序，尤其是在生产环境中。因此一些常用服务器管理工具都是基于服务器/客户端工作模式的。SuperScan 是基于面向连接式协议的 TCP 端口扫描器、pinger 和主机名解析器。针对任意 IP 地址范围的端口扫描和任意端口扫描。端口检测可以取得目标计算机提供的服务，同时也可以检测目标计算机是否有木马。可以看看端口检测的具体使用。

1. 检测目标计算机的所有端口

如果检测的时候没有特定的目的，只是为了了解目标计算机的一些情况，可以对目标计算机的所有端口进行检测，但是一般不提倡这种检测，原因有以下几种：

- 它会对目标计算机的正常运行造成一定影响，同时，也会引起目标计算机的警觉；
- 扫描时间很长；
- 浪费带宽资源，对网络正常运行造成影响。

01 在 IP 下输入起始和终止 IP，如 192.168.1.116。在扫描类型下选中“所有端口从”单选按钮，输入其范围，1～65 535，如果需要返回计算机的主机名，可以选中“查询计算机名”复选框，然后单击“开始”按钮，开始对一台目标计算机所有端口进行扫描，如图 12.24 所示。

02 扫描完成以后，单击“全部展开”按钮，可以看到扫描结果。显示如图 12.25 所示。

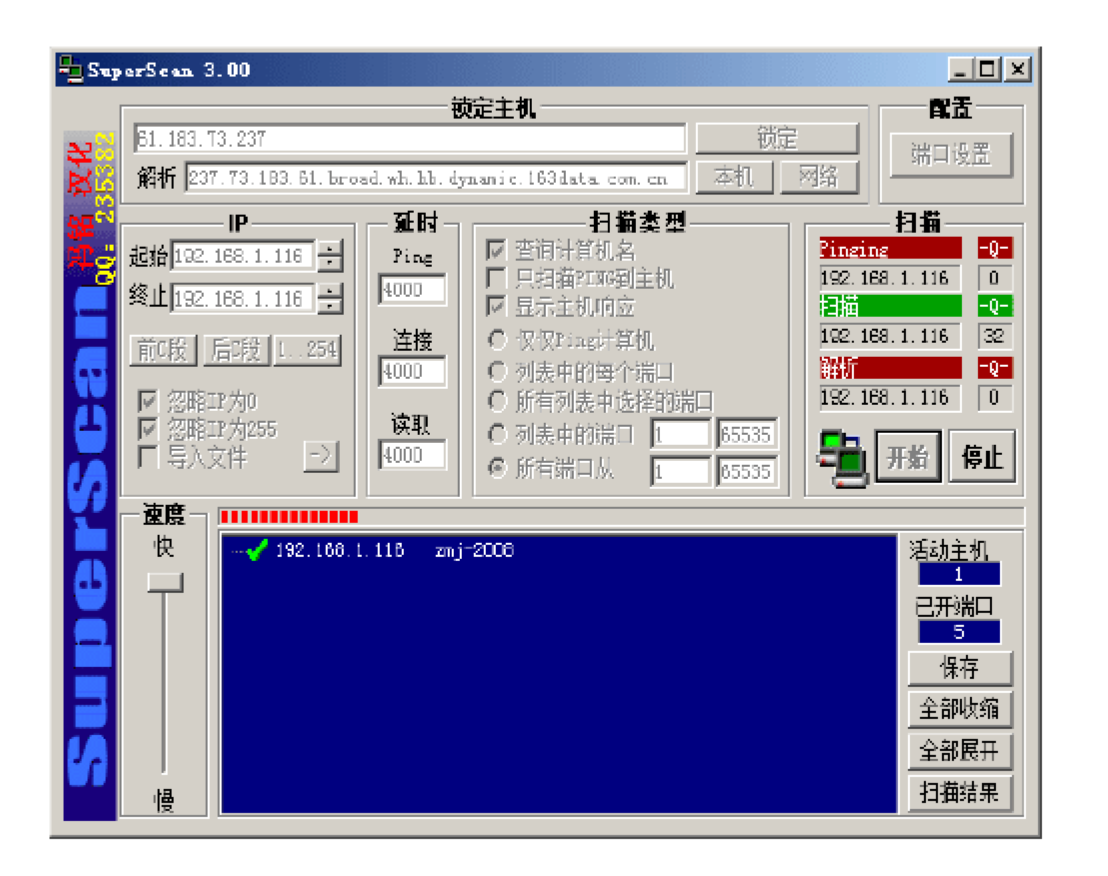


图 12.24　扫描目标计算机的所有端口



图 12.25　扫描结果

对扫描结果的描述如下：

- 第一行是目标计算机的 IP 和主机名；
- 第二行开始的小圆点是扫描的计算机的活动端口号和对该端口的解释；
- “活动主机”显示扫描到的活动主机数量，这里只扫描了一台，为 1；
- “已开端口”显示目标计算机打开的端口数，这里是 10。

2. 扫描目标计算机的特定端口

大多数时候不需要检测所有端口，只需检测有限的几个端口就可以了，主要是为了得到目标计算机提供的服务和使用软件的安全。所以，可以根据个人目的的不同来检测不同的端口，如：检测 80 端口、21 端口以及 23 端口，即使是攻击，也不会有太多的端口检测。

01 单击“端口设置”按钮，打开“编辑端口列表”界面，在“端口选择”下双击需要扫描的端口，如 21、23 以及 80 三个端口，这时端口前面会有一个“√”的标志，如图 12.26 所示。

02 单击“保存”按钮，显示如图 12.27 所示“Save port list file”对话框，输入文件名，如“端口 1”。单击“确定”按钮，保存选择的端口。



图 12.26　选择端口号

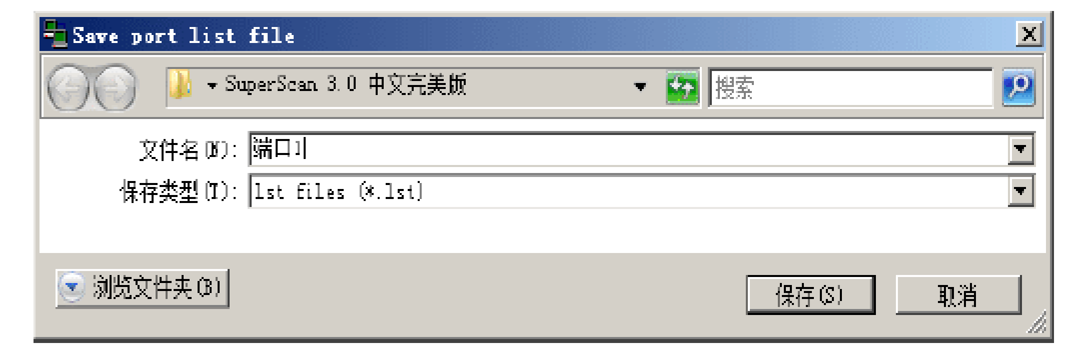


图 12.27　“Save port list file”对话框

03 选择保存路径，继续单击“保存”按钮。切换至“编辑端口列表”界面，单击“确定”按钮。

04 在“扫描类型”下选中“所有列表中选择的端口”单选按钮，单击“开始”按钮，对特定端口进行扫描，如图 12.28 所示。



图 12.28　对特定端口扫描结果

使用自定义端口的方式有以下优点：

- 选择端口时可以详细了解端口信息；
- 选择的端口可以自己取名保存，有利于再次使用；
- 可以根据要求有的放矢地扫描目标端口，节省时间和资源；
- 根据一些特定端口，可以扫描目标计算机是否被攻击者利用，或者打开不应该打开的服务。

12.4　关闭端口

通过运行端口查看工具，不难发现系统中的许多端口默认都是开启的，为了确保系统和网络的安全，必须将可能存在安全风险的端口及时关闭。例如，最常见的 RPC 服务的 TCP 端口 135、139、445、593、1025 和 UDP 端口 123、137、138、445、1900，以及远程服务访问端口 3389 等。

12.4.1　关闭常用端口

按照默认设置安装的 Windows Server 2008，安装完成后会自动开放许多端口，都是为了满足日常管理和维护而设置的，但是对系统安全却是一种无形的隐患，如共享功能开启的 139、445 端口等。为此，管理员可以根据需要对端口进行控制。

1. 关闭 23 端口

23 端口主要用于 Telnet（远程登录）服务，是 Internet 上普遍采用的登录和仿真程序。利用 Telnet 服务，黑客可以搜索远程登录的服务，扫描操作系统的类型。对系统的漏洞进行攻击，所以建议关闭 23 端口。

01 选择“开始”→“管理工具”→“服务”命令，显示如图 12.29 所示“服务”窗口。

02 在右侧窗格中双击“Telnet”选项，打开如图 12.30 所示“Telnet 的属性（本地计算机）”对话框，在“启动类型”处选择“手动”选项，单击“停止”按钮，再单击“确定”按钮，完成设置。

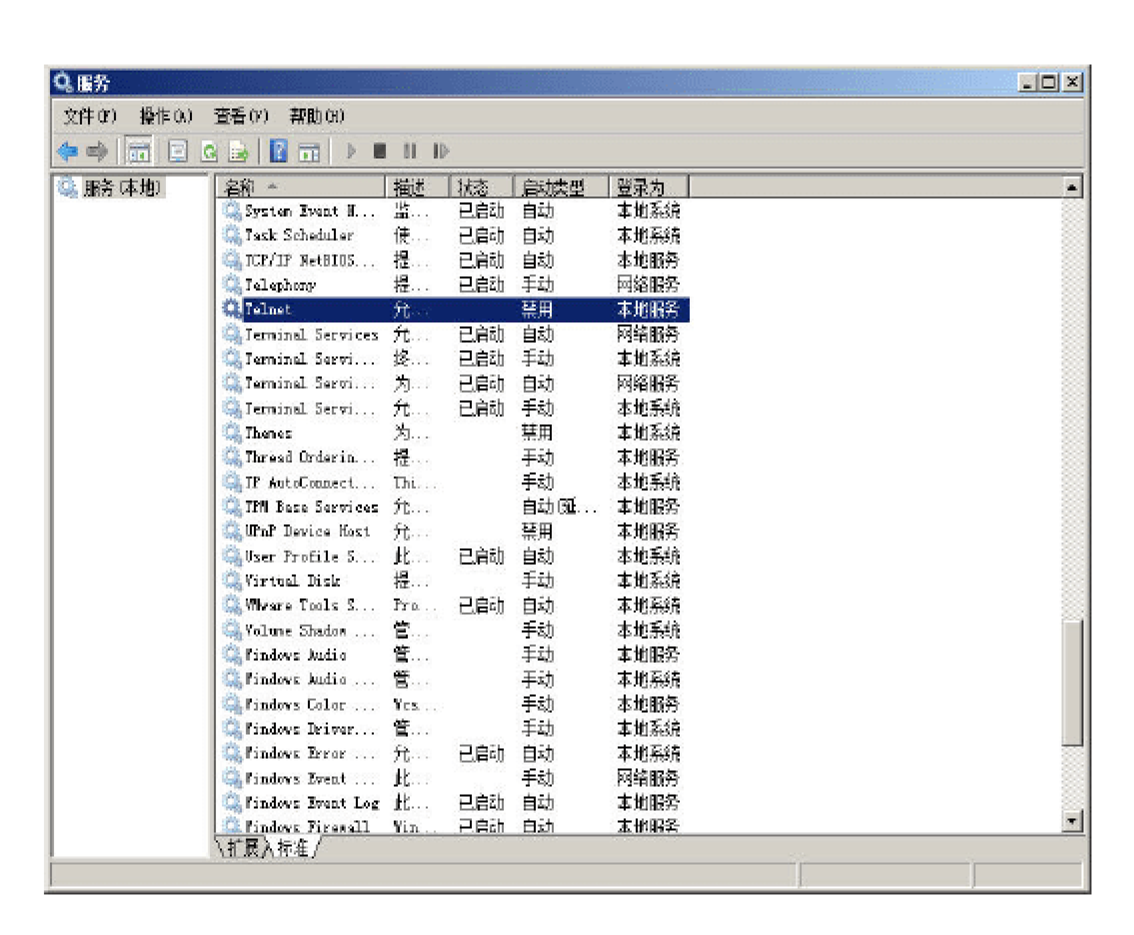


图 12.29 “服务”窗口

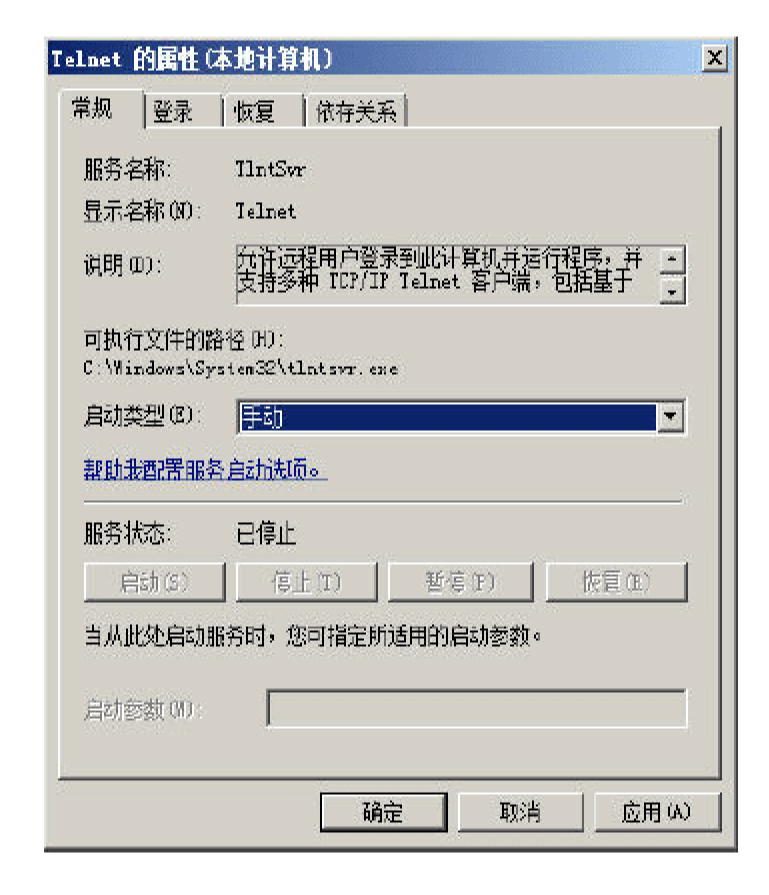


图 12.30 “Telnet 的属性（本地计算机）”对话框

2. 关闭 135 端口

通过 135 端口，可以远程随意控制计算机的上网情况，包括偷窥上网账号，监控浏览内容等。如此一来，开通服务器的 135 网络端口，很有可能招来各种恶意的远程攻击，为确保网络服务器的安全，关闭 135 网络端口是很有必要的。

01 选择“开始”→“运行”命令，打开如图 12.31 所示“运行”对话框，在文本框中输入“dcomcnfg”命令，单击“确定”按钮，打开“组件服务”窗口。

02 依次选择“控制台根节点”→“组件服务”→“计算机”选项，右击“我的电脑”选项，选择快捷菜单中的“属性”选项，显示如图 12.32 所示“我的电脑 属性”对话框，选择“默认属性”选项卡，取消“在此计算机上启用分布式 COM（E）”复选框。

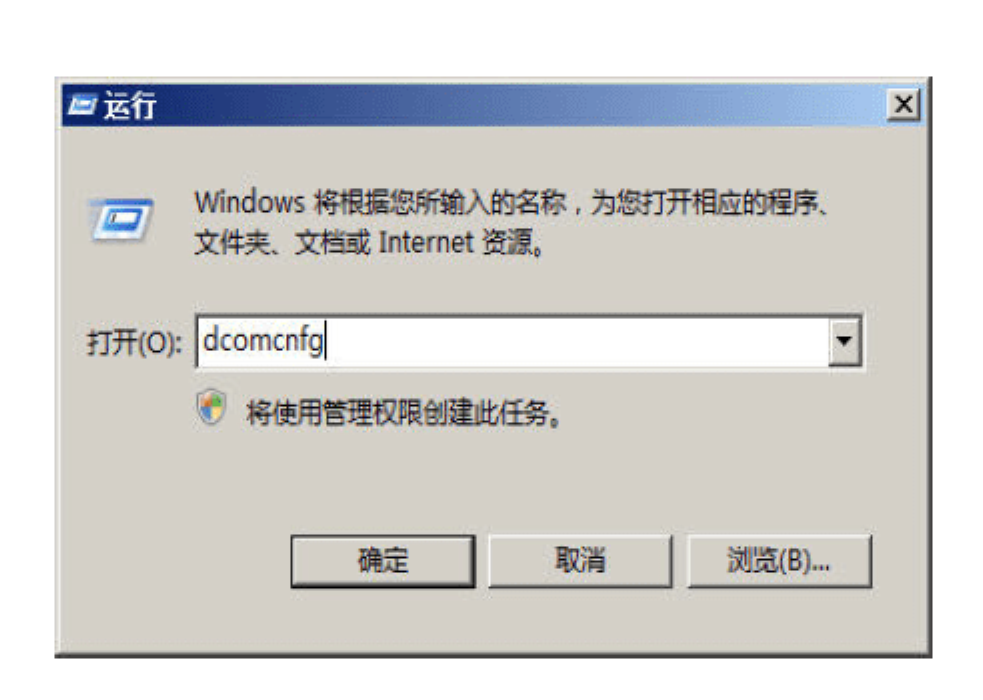


图 12.31 “运行”对话框

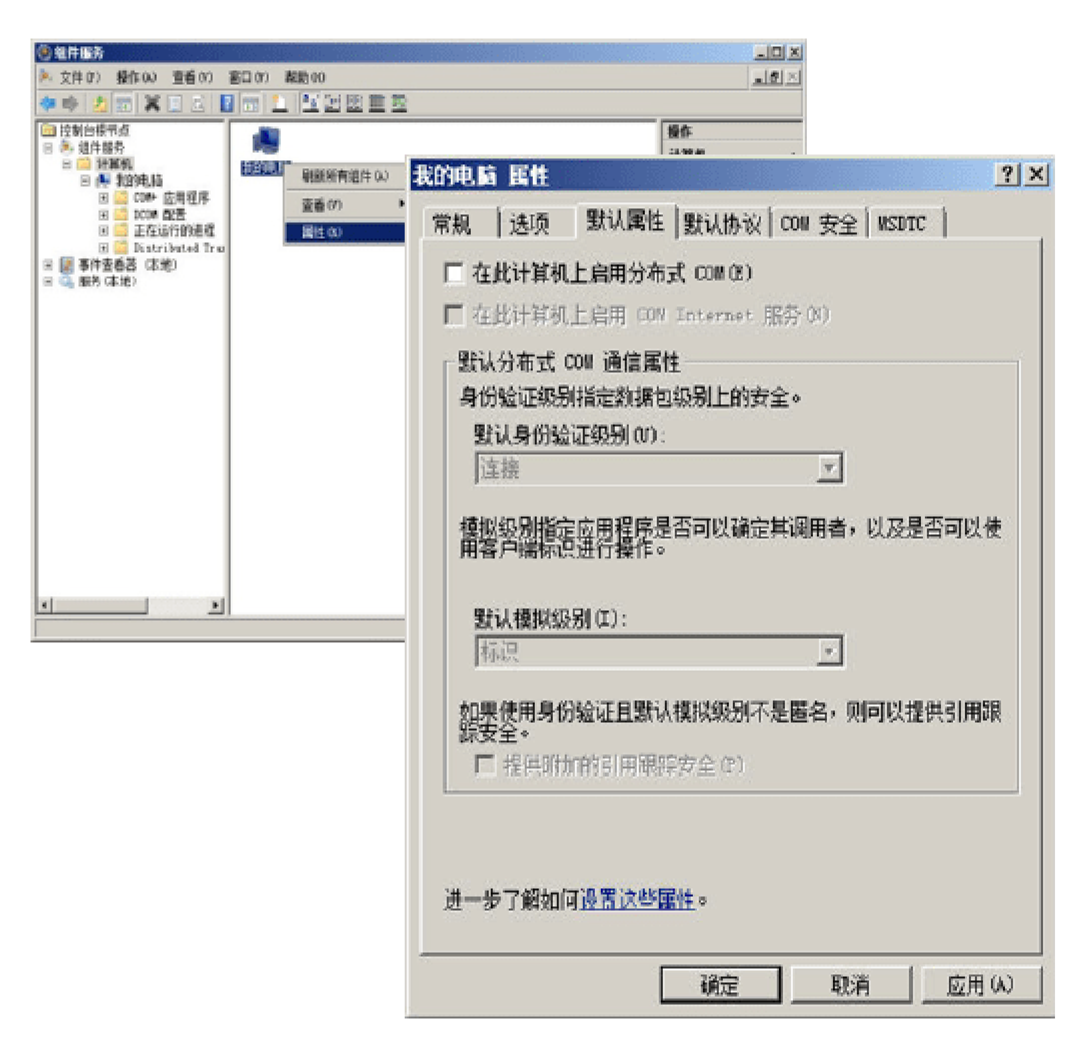


图 12.32 “我的电脑 属性”对话框

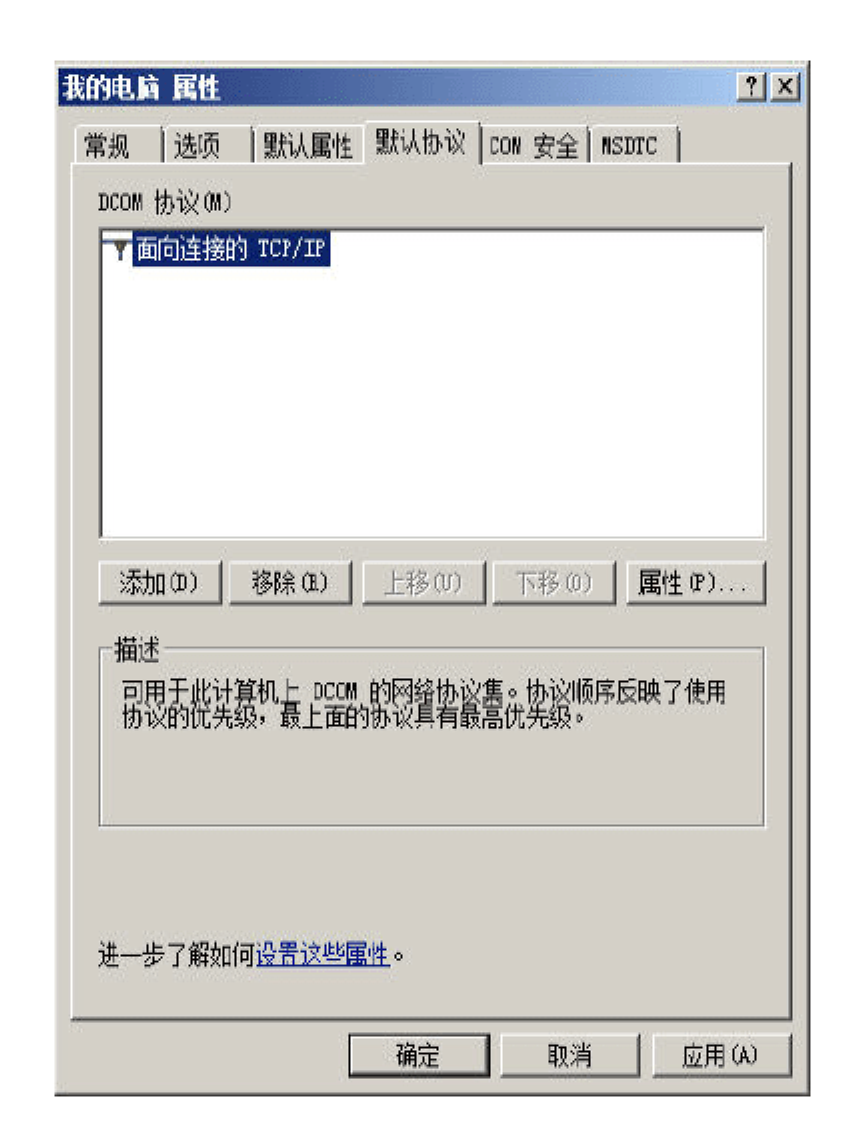


图 12.33　“默认协议”选项卡

03 选择“默认协议”选项卡，选中“面向连接的 TCP/IP”，单击“移除”按钮，显示如图 12.33 所示。

04 单击“确定”按钮，设置完成，重新启动后即可关闭 135 端口。

3. 关闭 139 端口

开启 139 端口虽然可以提供共享服务，但是经常被攻击者所利用进行攻击，因此如果用户不需要共享文件时，应及时关闭 139 端口。

01 打开“网络和共享中心”窗口，单击“查看状态”链接，显示“本地连接 状态”对话框，单击“属性”按钮，显示“本地连接 属性”对话框，双击“Internet 协议版本 4（TCP/IPv4）”选项，显示“Internet 协议版本 4（TCP/IPv4）属性”对话框，如图 12.34 所示。

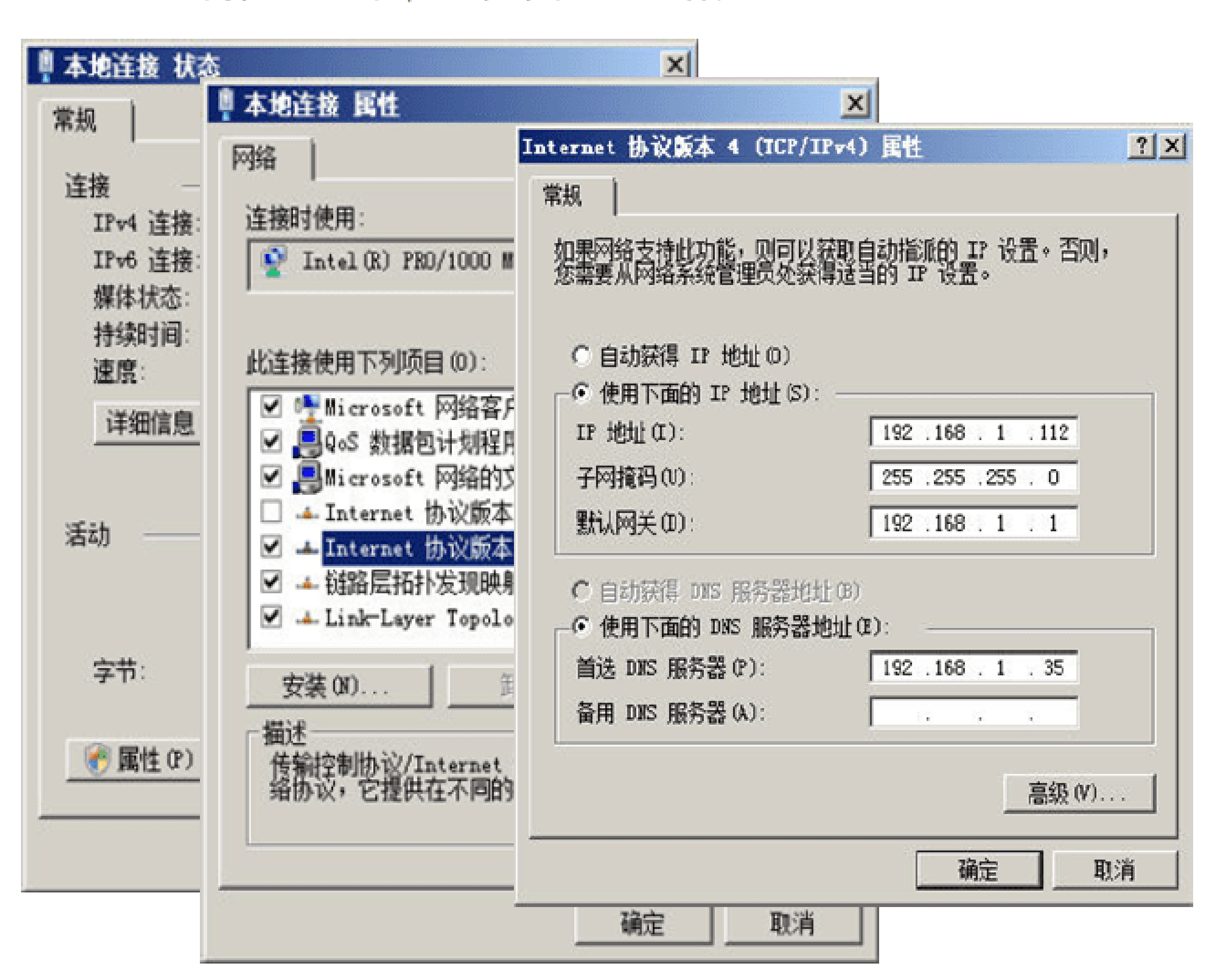


图 12.34　打开“Internet 协议版本 4（TCP/IPv4）属性”对话框

02 单击“高级”按钮，显示如图 12.35 所示“高级 TCP/IP 设置”对话框，选择“WINS”选项卡，在“NetBIOS 设置”下选中“禁用 TCP/IP 上的 NetBIOS（S）”单选按钮，单击“确定”按钮，保存设置即可。

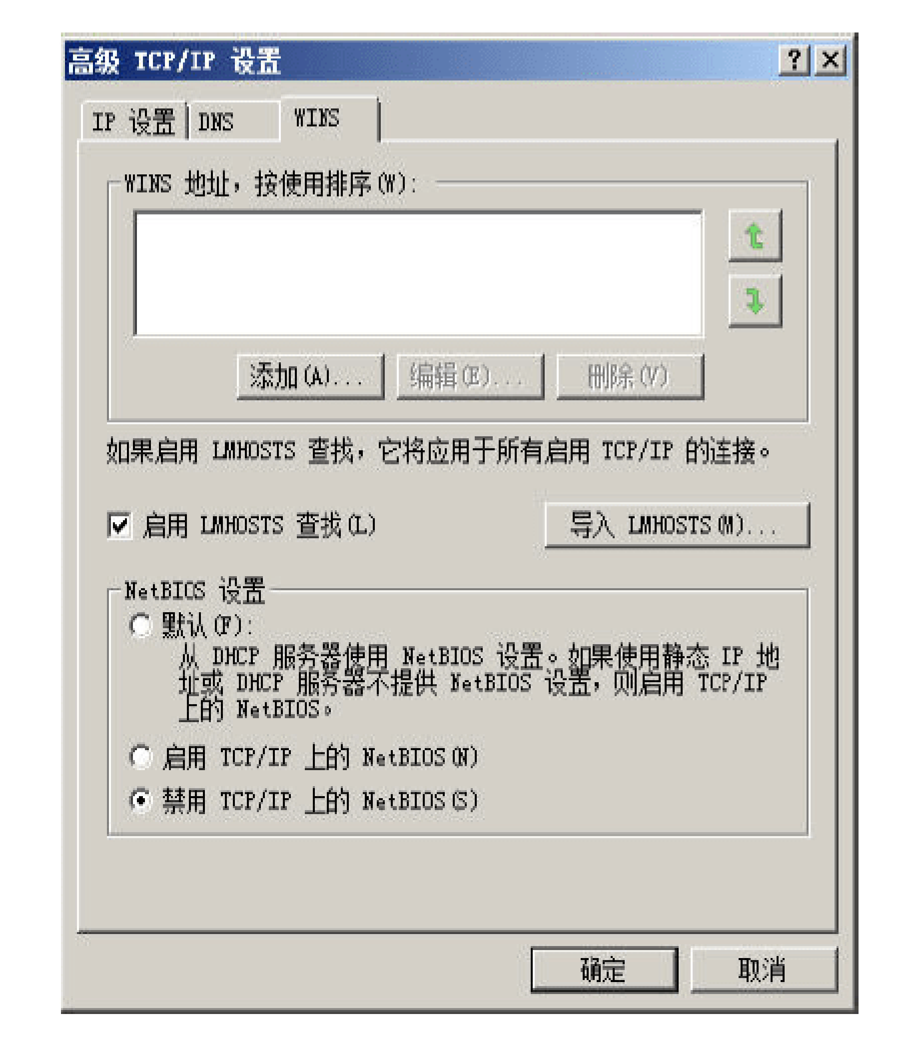


图 12.35 “高级 TCP/IP 设置”对话框

4. 关闭 445 端口

开启 445 端口用户可以在局域网中轻松访问各种共享文件夹或共享打印机，这样一来，其问题也随之产生，有了 445 端口，黑客们有机可承，通过该端口偷偷共享用户的硬盘，甚至会在悄无声息中将用户硬盘格式化掉。为此用户所能做的就是想办法不让黑客有机可乘，封堵住 445 端口漏洞。

01 选择“开始”→“运行”命令，打开“运行”对话框，在文本框中输入“regedit”字符串命令，单击“确定”按钮，打开“注册表编辑器”窗口。依次展开 KEY_LOCAL_MACHINE→SYSTEM→ControlSet→Services→NetBTParameters 选项。

02 右击“Parameters”选项，在弹出的快捷菜单中选择“新建”→“DWORD（32-位）值”选项。将 DWORD 值命名为“SMBDeviceEnabled”。右击“SMBDeviceEnabled”值，选择快捷菜单中的“修改”选项，显示如图 12.36 所示“编辑 DWORD（32 位）值”对话框，在“数值数据”文本框中输入“0”，单击“确定”按钮，完成设置。

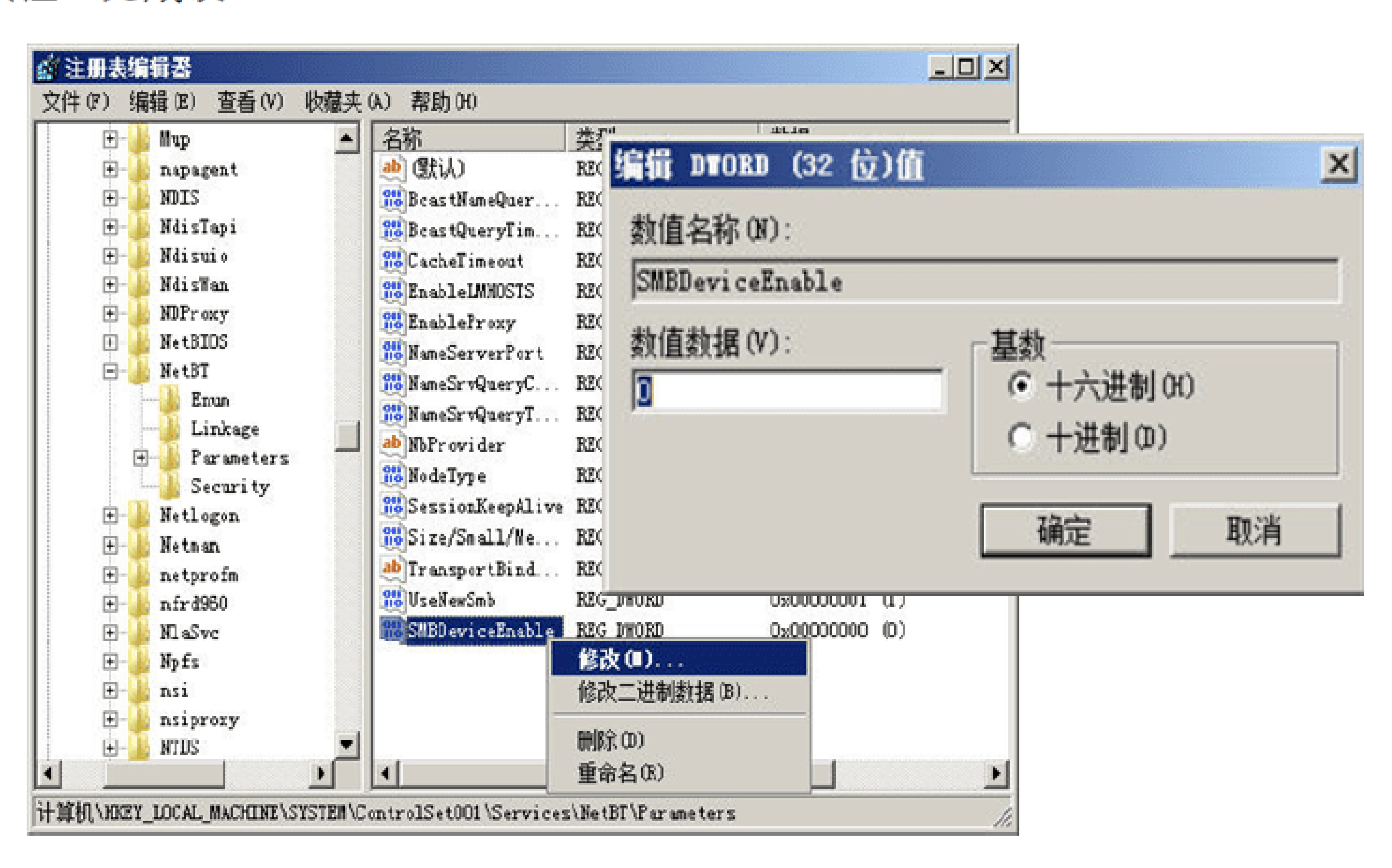


图 12.36 打开“编辑 DWORD（32 位）值”对话框

12.4.2　IPSec 禁用端口

利用 IPSec 实现对开放端口的禁用，如 135 端口和 445 端口，这两个端口都与共享有很大的关系，如果这两个端口禁用的话将会导致共享功能无法进行。针对微软系统而言端口的开放是必然的，但是开放了不必要的端口又是很危险的，所以很矛盾，为了能够有效的保证计算机系统的安全，建议大家将不必要的端口实现禁用操作。

01 使用“netstat -an”命令，查看本地计算机中打开了哪些端口，如图 12.37 所示。

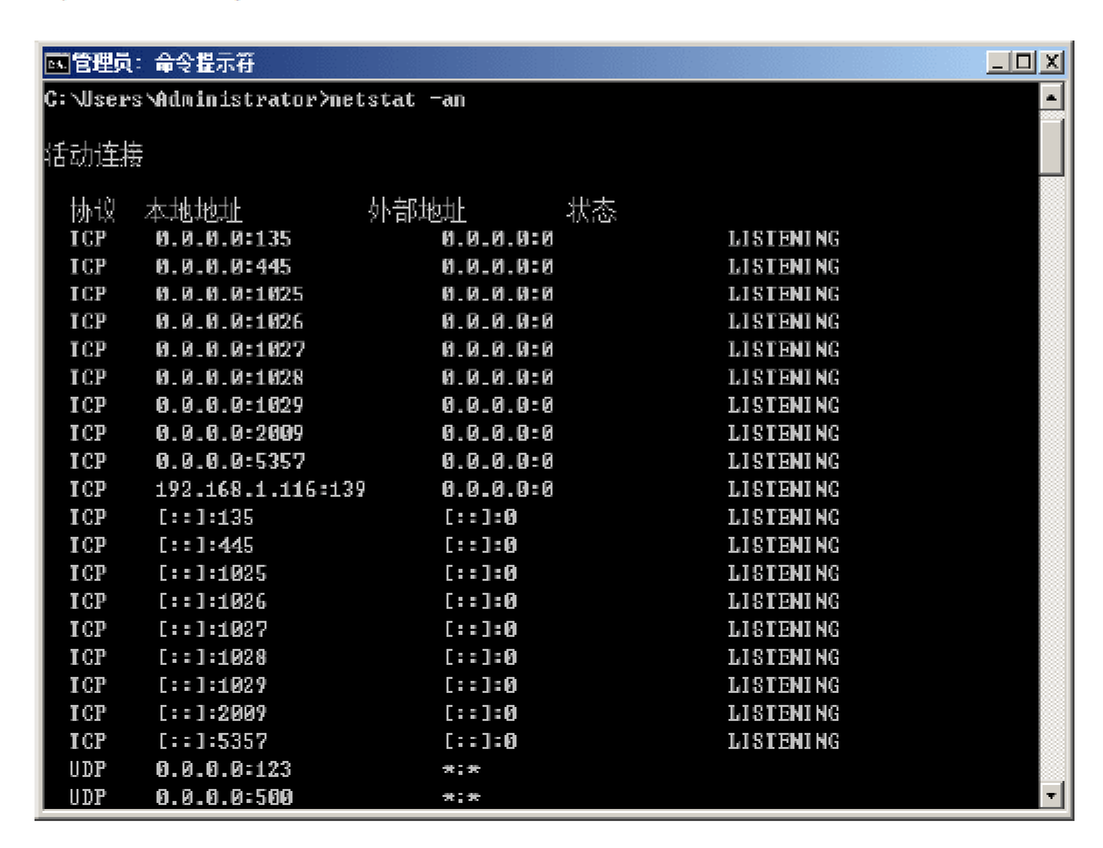


图 12.37　Netstat –an 属性

02 依次选择“开始”→“管理工具”→“本地安全策略”命令，打开“本地安全策略”窗口。右击“IP 安全策略，在本地计算机”选项，选择快捷菜单中的“创建 IP 安全策略”命令，启动“IP 安全策略向导”。依次单击“下一步”按钮，设置 IP 策略名称和安全通信请求，如图 12.38 所示。

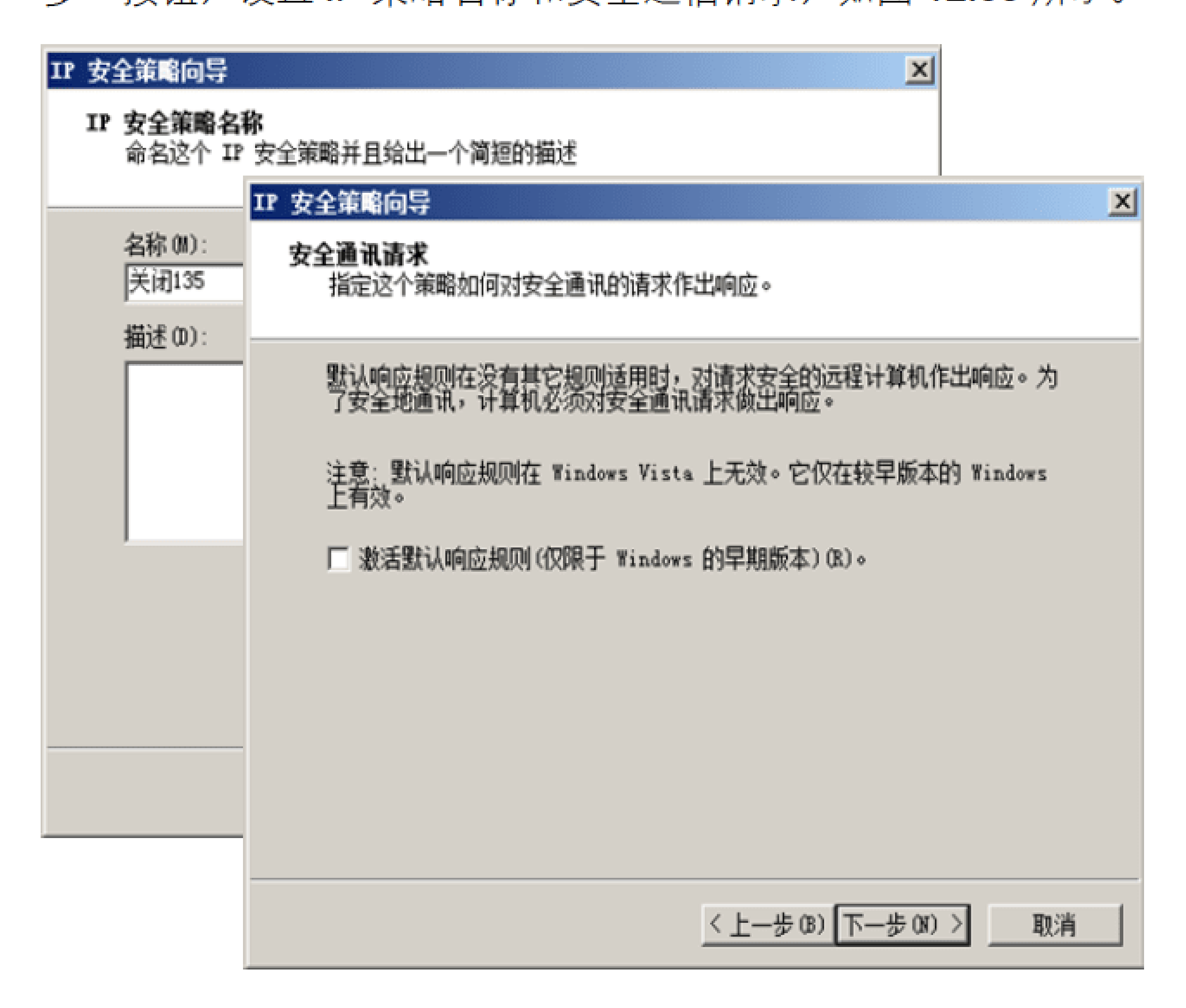


图 12.38　IP 安全策略名称和安全通讯请求

03 单击“下一步”按钮，进入“正在完成 IP 安全策略向导”对话框，单击“完成”按钮创建了一个新的 IP 安全策略。右击该 IP 安全策略，选择“属性”选择，显示“关闭 135 属性”对话框，取消“使用添加向导”

复选框，单击“添加”按钮，显示“新规则属性”对话框，添加新的规则。单击“添加”按钮，显示“IP 筛选器列表”对话框，输入名称，如 close 135，取消“使用添加向导”复选框，如图 12.39 所示。

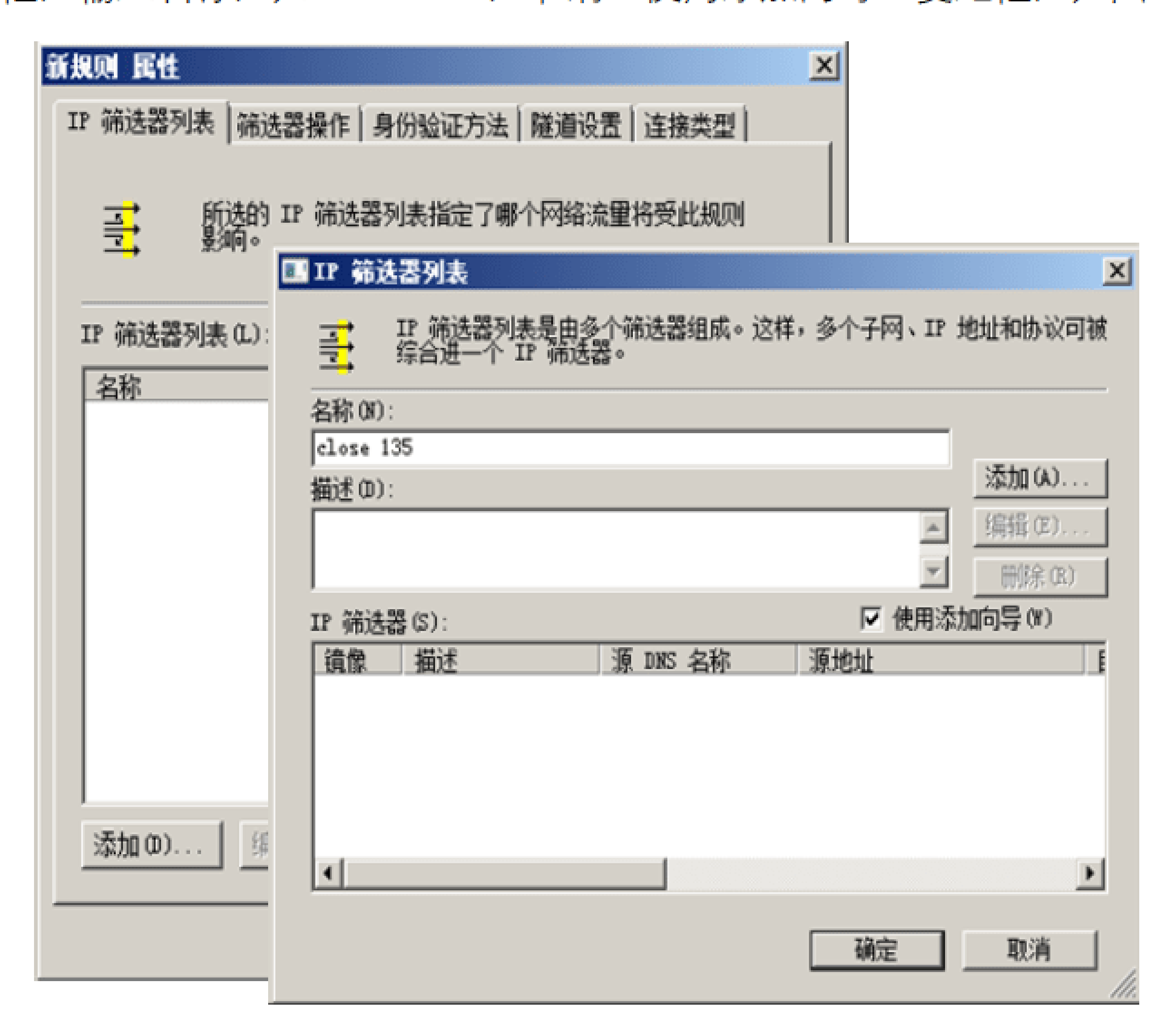


图 12.39　新规则属性和 IP 筛选器列表

04 单击“添加”按钮，显示如图 12.40 所示“IP 筛选器 属性”对话框，在“源地址”下拉列表中选择“任何 IP 地址”选项，在“目标地址”的下拉列表中选择“我的 IP 地址”选项。选择“协议”选项卡，在“选择协议类型”的下拉列表中选择“TCP”选项，在“到此端口”下的文本框中输入“135”，单击“确定”按钮，即可添加了一个屏蔽 TCP135 端口的筛选器，能够防止外界通过 135 端口连上本地计算机。

05 单击“确定”按钮，返回到“新规则属性”对话框，选中“IP 筛选器列表”下名称为“close 135”单选按钮，其左边的圆圈上加一个点，表示已经激活。

06 切换到“筛选器操作”选项卡，取消“使用添加向导”复选框，单击“添加”按钮，显示如图 12.41 所示“新筛选器操作 属性”对话框，选择“安全方法”选项卡，选中“阻止”单选按钮。



图 12.40　设置“IP 筛选器 属性”

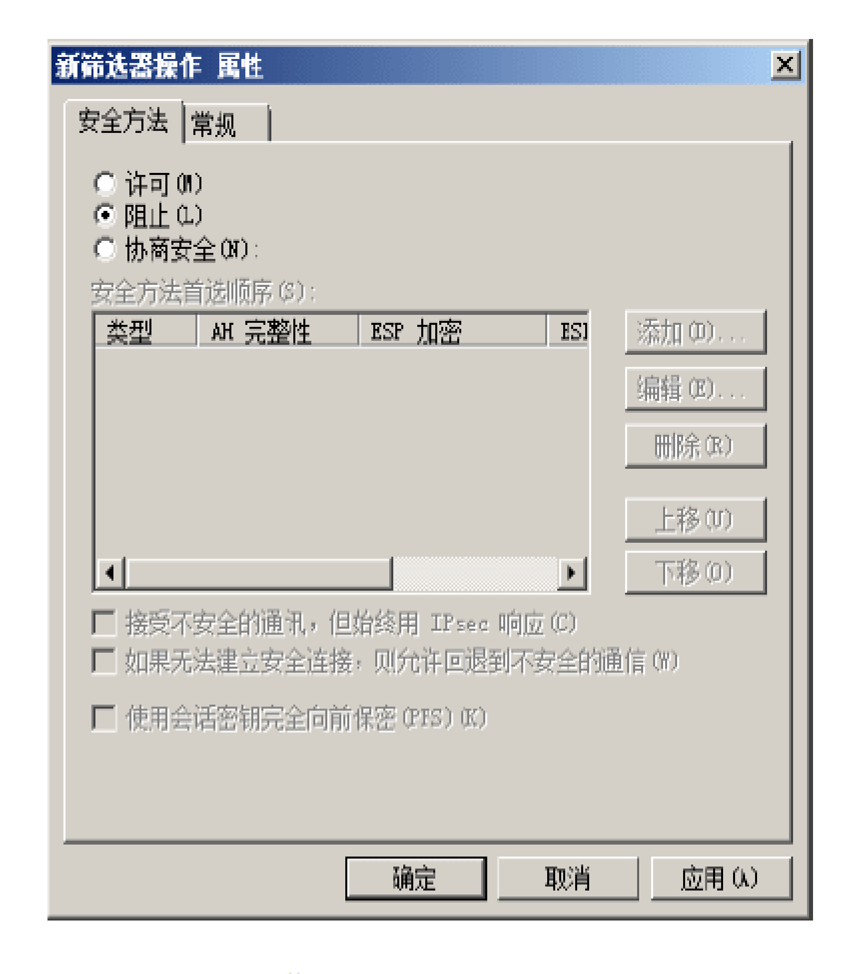


图 12.41　“新筛选器操作 属性”对话框

07 单击“确定”按钮，显示如图 12.42 所示“新规则 属性”对话框，选中“新筛选器操作”单选按钮，单击“关闭”按钮关闭对话框。单击“确定”按钮，保存设置。在“本地安全策略”窗口，右击新添加的 IP 安全策略，选择快捷菜单中的“分配”命令，即可分配该新建策略。

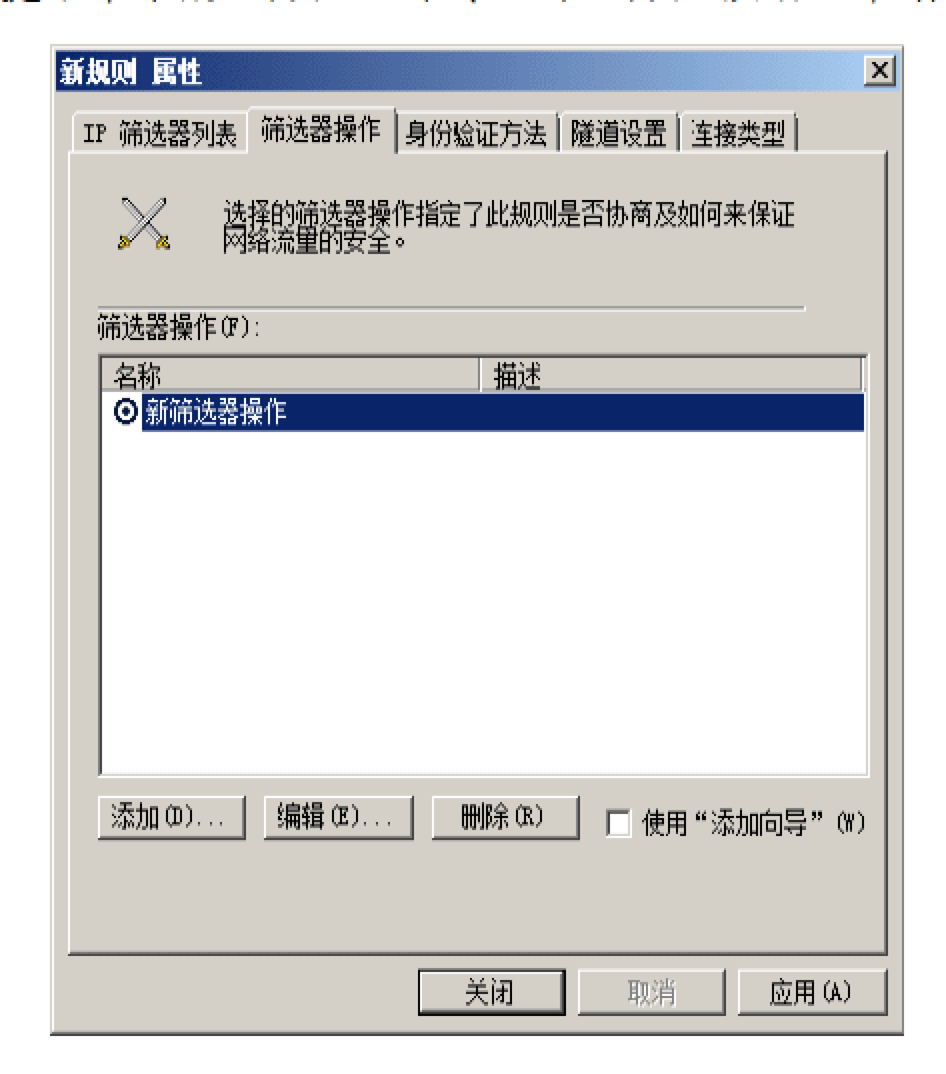


图 12.42　“新规则 属性”对话框

08 重新启动计算机，主机上设置好的端口被关闭，病毒和黑客将连不上这些端口，从而保护计算机的安全。

12.4.3　关闭服务

网络服务是通过操作系统中的端口向网络用户提供的，并且一种网络服务可能同时需要多个端口，关闭服务即可关闭相应的端口。以关闭 Windows Server 2008 系统的 FTP 服务为例，介绍如何通过这种方法配置 Windows 端口。

01 依次选择“开始”→“管理工具”→“服务”命令，显示“服务”窗口。双击“FTP Publishing Service”服务，显示如图 12.43 所示“FTP Publishing Service 的属性”对话框。如果安装了 FTP 服务，此服务将随系统启动而自动运行。

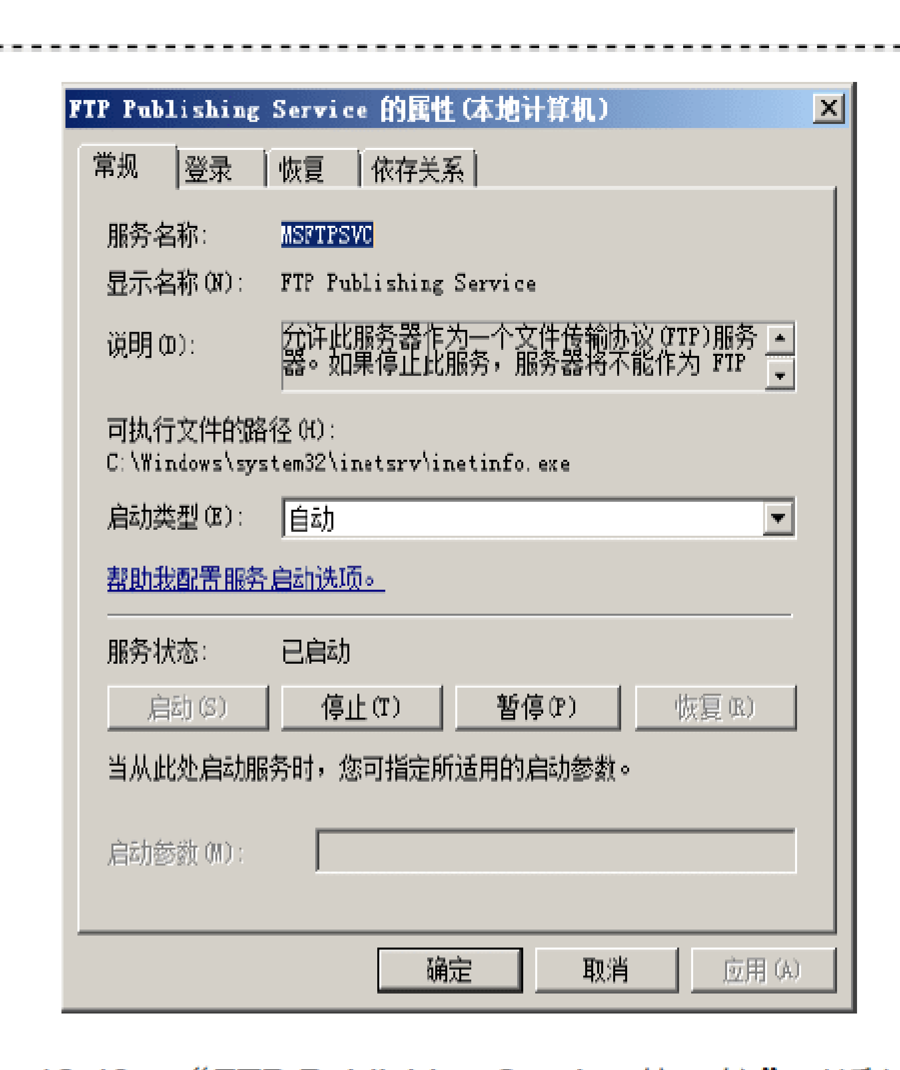


图 12.43　“FTP Publishing Service 的属性”对话框

02 单击“停止”按钮，停止该服务，然后在“启动类型”下拉列表中选择“禁用”，如图 12.44 所示。



图 12.44 “常规”选项卡

03 单击“确定”按钮，即可关闭 FTP 服务对应的端口。

如果要开启该端口，只需先在“启动类型”选择“自动”选项，单击“应用”按钮，然后单击“启动”按钮即可。

12.5 重定向默认端口

常用网络服务的默认端口是众所周知的，通过端口重定向可以改变服务器的默认设置，绕过入侵者对常规设置的攻击。例如，3389 端口是 Windows Server 2008 远程桌面的服务端口，可以通过这个端口，用“远程桌面连接”工具连接到远程的服务器，如果连接上，输入系统管理员的用户名和密码后，将变得可以像操作本机一样操作远程计算机。为了确保远程终端连接的安全性，可以将其默认端口调整为 2009 或其他。

01 打开“注册表编辑器”窗口，依次选择 HKEY_LOCAL_MACHINE→SYSTEM→CurrentControlSet→Control→Terminal Server→Wds→rdpwd→Tds→tcp 选项（如果无法找到时可以自行创建），显示如图 12.45 所示“注册表编辑器”窗口。

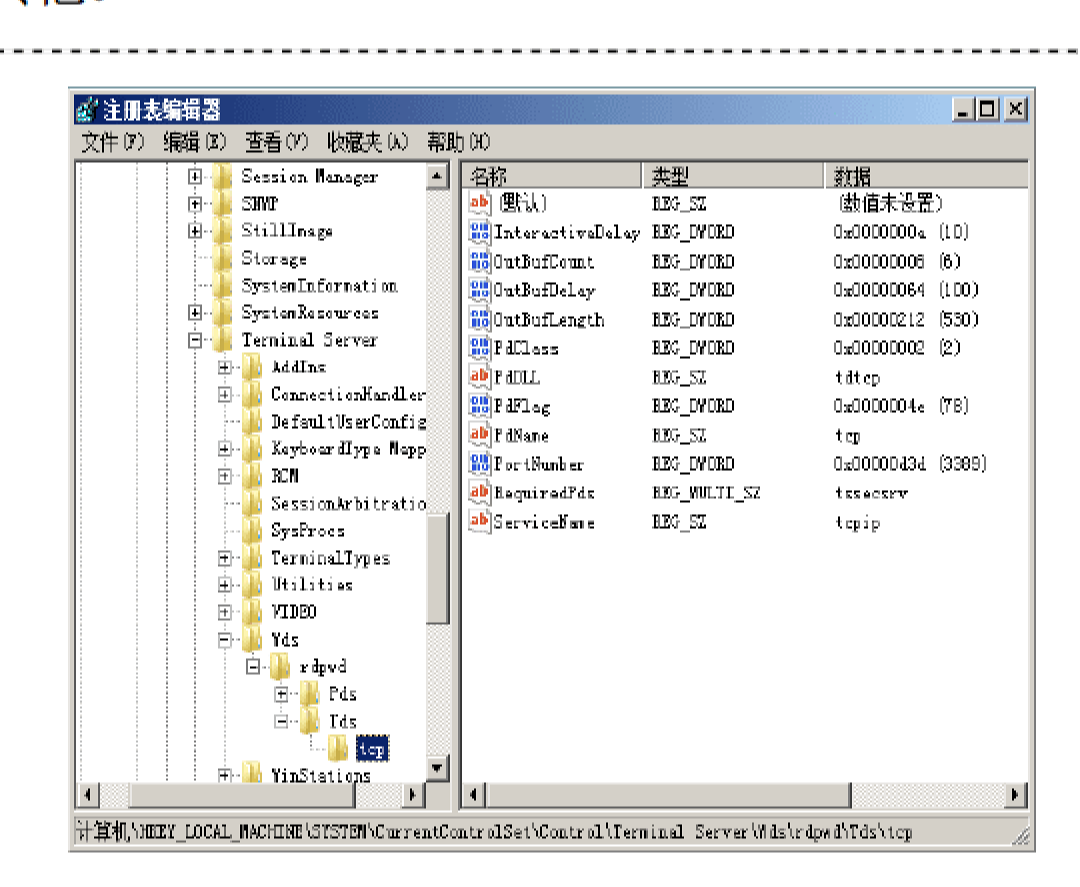


图 12.45 tcp 注册表子项

02 在目标注册表子项中，双击 PortNumber 选项，显示如图 12.46 所示“编辑 DWORD（32 位）值”对话框。在数值数据中输入“2009”，单击“确定”按钮。

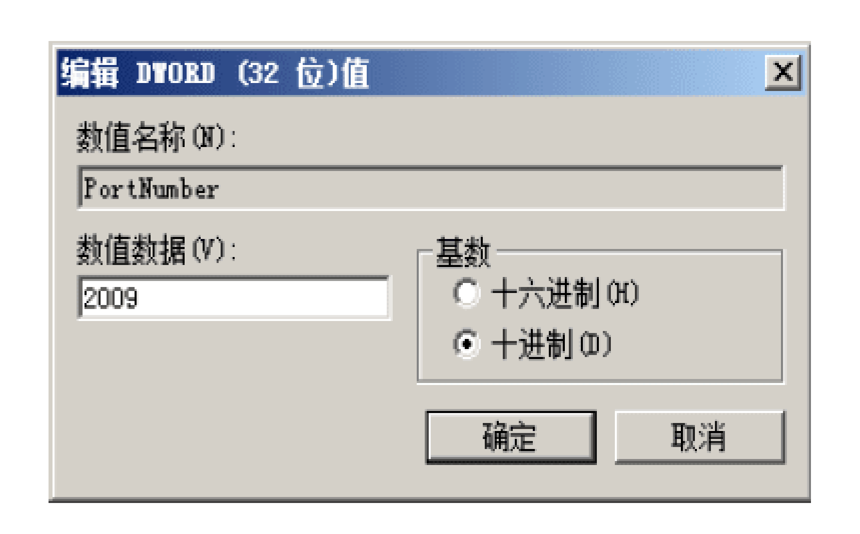


图 12.46　“编辑 DWORD（32 位）值”对话框



03 在“注册表编辑器”窗口中，依次展开“HKEY_LOCAL_MACHINE → HKEY_LOCAL_MACHINE → SYSTEM → CurrentControlSet → Control → TerminalServer → WinStations→RDP-Tcp”选项，如图 12.47 所示。双击“PortNumber”选项，在数值数据中输入“2009”，单击“确定”按钮退出 Windows Server 2008 系统注册表编辑器窗口，重新启动，就可以使上述设置操作正式生效。

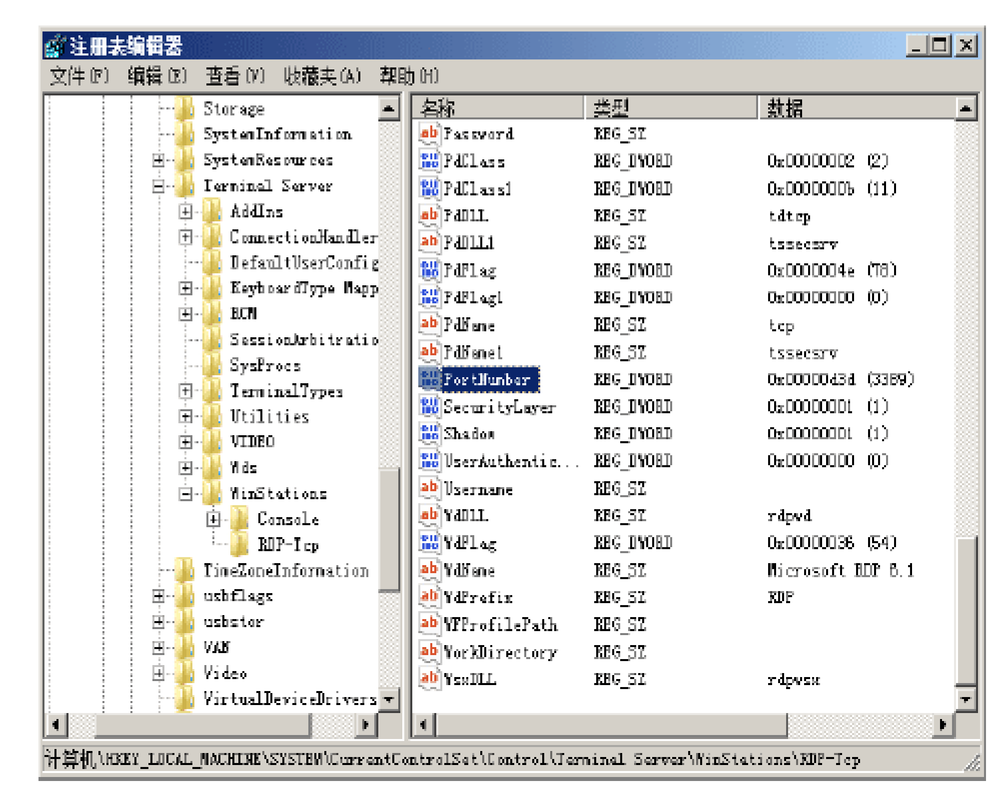


图 12.47　RDP-Tcp 注册表子项

04 在远程终端计算机上，依次选择“开始”→“所有程序”→“附件”→“远程桌面连接”命令，在“远程桌面连接”对话框中，输入要远程连接的“计算机名：2009”或“IP 地址：2009”，如 192.168.1.116：2009，如图 12.48 所示。单击“确定”按钮，输入帐户和密码，即可远程连接到计算机上。



图 12.48　“远程桌面连接”对话框

注意



在更改远程桌面访问端口后，一定要检查一下防火墙是否会拦截该端口，一定要将此新端口加入防火墙允许的范围。

小　结

端口安全是系统安全中最容易被忽视的“角落”，其实，监听和分析端口往往是黑客入侵系统的第一步，此时，如果管理员可以觉察到端口状态的变化，便有机会挫败黑客的入侵。端口分类的依据主要有两种：端口号和协议类型。为了便于系统管理，用户应该熟知一些常用端口，并且掌握几种最常用的端口查看工具。默认情况下，许多端口都是开启的，而对于一些高风险的端口必须及时关闭。关闭端口的方法有多种，最常用的就是 IPSec 禁用端口和关闭服务。

另外，对于计算机默认的端口，如端口 3389 等，建议采用重定向方式，确保服务器的安全。

习　　题

1. 端口在计算机中起什么作用？
2. 在上网的时候，常用的端口有哪些？
3. 如何使用 netstat 命令查看端口？
4. 如何重定向本机的默认端口、保护本地计算机的安全？

实验：查询和配置端口

实验目的

掌握查询端口状态的操作，并且根据需要开启和关闭端口。

实验内容

端口 445 是一种 TCP 端口，提供局域网中文件或打印机共享服务。该端口是基于 CIFS 协议工作的。攻击者与 445 端口建立请求连接，也能获得指定局域网内的各种共享信息。因此，可以先使用 netstat 命令查询一下 445 端口的状态，如果开启，则将其关闭。

实验步骤

1. 查询 445 端口状态。
2. 创建新的 IP 安全策略。
3. 添加新的规则。
4. 屏蔽 TCP 135 端口。
5. 激活新筛选器操作。
6. 在主机上设置端口。

第13章

审核策略与事件日志

自 Windows NT 以来，安全事件日志就是令系统管理员头疼不已，而又不得不经常面对的问题。事件日志中包含了许多有关系统运行状态、安全策略、用户行为等的重要信息，但是对审核策略缺乏合理的控制，使得管理员不得不从海量的历史事件日志中，查找自己真正需要的信息。在 Windows Server 2008 中，审核系统有了很大的改进，使用起来更加方便。审核策略的扩充，使用户可以更加方便地选择要查看的事件。审核事件记录格式和内容也有所变化，用户能够更容易在安全日志中了解事件。

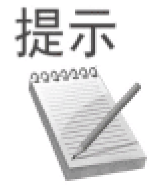
本章导读

- 审核策略的设置，启用与优化
- Windows Server 2008 中的新事件
- 系统日志的分析，设置与调试

Windows Server 2008

13.1 审核策略

审核是 Windows Server 2008 系统安全策略的一部分。通过设置审核策略，确定是否将安全事件记录到计算机上的安全日志中，同时也确定是否记录登录成功或登录失败，或二者都记录。系统管理员希望了解系统运行状态时，通过查看相关类型的系统事件即可，相对于大量的系统时间信息而言，审核策略产生的日志数量就非常小了，大大节约了查看时间。

提示  在加入域中的成员服务器和工作站上，默认情况下未定义事件类别的审核设置。在域控制器上，默认情况下审核关闭。通过为特定的事件类别定义审核设置，可以创建一个适合组织安全需要的审核策略。

13.1.1 审核策略概述

安全访问控制策略包括 3 项基本控制，即认证、授权和审核。认证是访问控制的“第一关”，负责验证对方身份的有效性，如用户名、密码等；授权是确认用户身份后，为其分配哪些访问权限，避免由于越界访问带来的安全隐患；审核则是记录用户访问过程中执行了哪些操作，是否对系统安全或网络安全构成威胁，并生成相应日志。审核策略只能跟踪检查用户的操作是否违规，以及是如何违规的，但并不能防止违规事件的发生。

1. Windows 审核的工作原理

Windows 审核系统、安全决策组件和事件日志服务配合工作，以可靠的方式为正在运行的网络服务生成安全事件。安全决策组件通常被称为安全参考监控，当制定了安全决策后，监视器就会通知审核系统，并将活动的细节传输到审核系统。审核系统将这些细节按照指定的格式生成事件日志，确保数据以连续形式显示，并且清除所有审核策略不允许日志的事件，其余事件被发送到事件日志服务，储存于安全日志中。如图 13.1 所示是 Windows 审核子系统的工作概况。

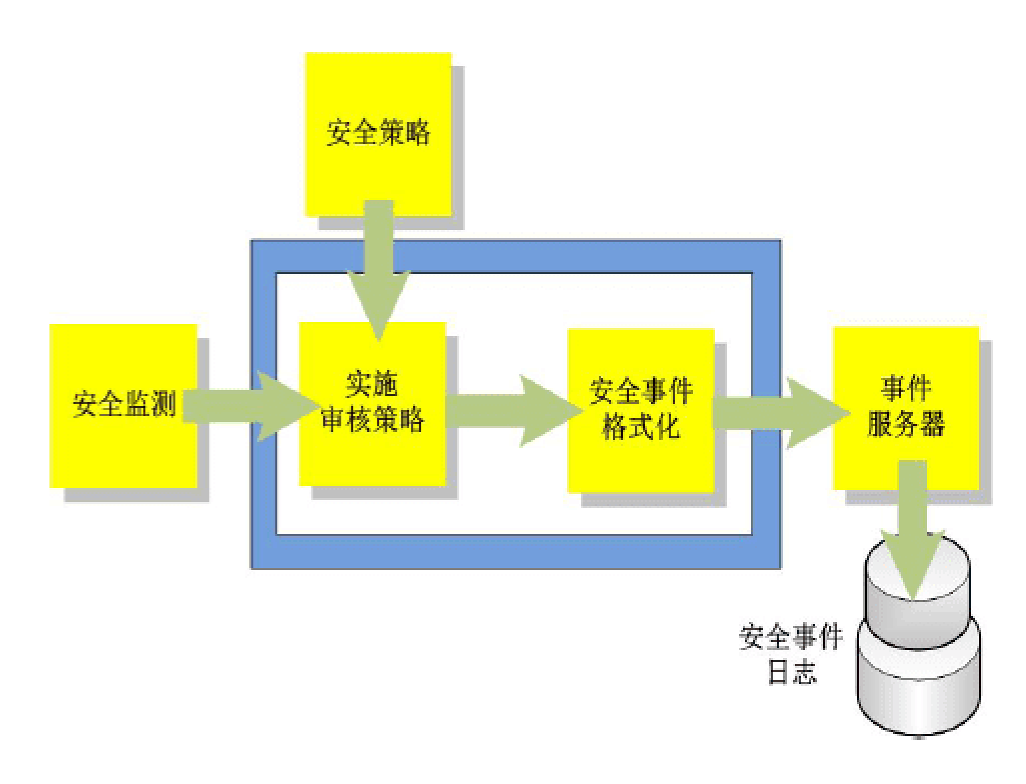
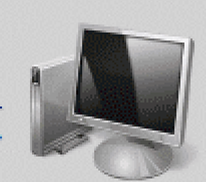


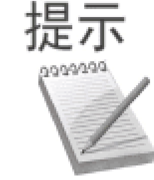
图 13.1 Windows 审核系统





注意　Windows 审核在为审核系统提供事件前，会检查审核策略，预防发生不必要的执行障碍。

Windows 审核系统在 LSA 进程中执行，在 Windows 进程列表和 Windows 核心中显示为 lsass.exe。LSA 包含 Windows 用户模式组件，用于执行安全策略和其他安全功能，例如认证。有些组件如认证包，是位于 LSA 内部的，其将事件直接传递到审核系统。运行于 LSA 外的用户模式中的组件（如 ADDS），以及使用 Windows 审核 APIs 的应用程序，只能经由 PRC 将事件传递到 LSA。内核包含着一个普通的审核界面供核心组件使用。它还包含一个对象管理器，负责生成多数对象访问事件。事件可以通过内核事件跟踪引擎（ETW）传递到事件日志服务，也可以通过 RPC 传递。大多数生成于内核的事件直接传递到 ETW，但需要复杂的事件则需先传递到 LSA 进行格式化。LSA 将多数事件通过 ETW 传递到事件日志，只有在部分审核子系统失败时才使用 RPC 渠道。



提示　在 Windows Vista 和 Windows Server 2008 系统中，事件日志引擎已经升级到 6.0 版本。旧的事件日志服务最大的有效日志文件为 4GB（在 x86 的计算机上会更小些），而使用新版本引擎的日志文件可以超过一个 PB。旧日志的最大传输速率为每秒几千个事件，而新日志的传输速率为每秒上万个。

2. 系统审核类型

在 Windows Vista 之前，所有安全事件都属于 9 种审核策略之一。通过启用一个审核类别的成功或失败的审核，就启用了该类别的所有审核事件。在 Windows Server 2008 和 Windows Vista 中，所有安全事件都归属于一个审核策略子类别。当启用了某子类别的审核策略后，也就启用了所有属于该子类别的事件。每个子类别的设置中，既有启用由成功的活动生成的事件，也有启用由失败的事件生成的事件。

（1）审核帐户登录事件

审核帐户登录事件设置确定是否审核在这台计算机用于验证帐户时，用户登录到其他计算机或者从其他计算机注销的每个实例。当在域控制器上对域用户帐户进行身份验证时，将产生帐户登录事件。该事件记录在域控制器的安全日志中。当在本地计算机上对本地用户进行身份验证时，将产生登录事件。该事件记录在本地安全日志中，不产生帐户注销事件。

如果定义该策略设置，可以指定是否审核成功、审核失败，或根本不对事件类型进行审核。当某个帐户的登录成功时，成功审核会生成审核项。当某个帐户的登录失败时，失败审核会生成审核项。

（2）审核帐户管理

审核帐户管理设置确定是否审核计算机上的每一个帐户管理事件。帐户管理事件的例子包括：

- 创建、更改或删除用户帐户或组；
- 重命名、禁用或启用用户帐户；
- 设置或更改密码。

如果定义该策略设置，可以指定是否审核成功、审核失败，或根本不对事件类型进行审核。任何帐户管理事件成功时，成功审核都会生成审核项。任何帐户管理事件失败时，失败审核都会生成审核项。

（3）审核目录服务访问

审核目录服务访问设置确定是否审核用户访问那些指定自己的系统访问控制列表（SACL）的 Active Directory 对象的事件。

默认情况下，在“默认域控制器组策略对象（GPO）”中该值设置为无审核，并且在该值没有任何意义的工作站和服务器中，它保持未定义状态。

如果定义该策略设置，可以指定是否审核成功、审核失败，或根本不对事件类型进行审核。用户成功访问指定了 SACL 的 Active Directory 对象时，成功审核会生成审核项。用户尝试访问指定了 SACL 的 Active Directory 对象失败时，失败审核会生成审核项。

注意 

通过使用某个 Active Directory 对象“属性”对话框中的“安全”选项卡，可以设置该对象的 SACL。该操作与审核对象访问相同，只不过仅应用于 Active Directory 对象而不是文件系统和注册表对象。

（4）审核登录事件

审核登录事件设置确定是否审核每一个登录或注销计算机的用户实例。

在域控制器上将生成域帐户活动的帐户登录事件，并在本地计算机上生成本地帐户活动的帐户登录事件。如果同时启用帐户登录和帐户审核策略类别，那么使用域帐户的登录将生成登录或注销工作站或服务器的事件，而且将在域控制器上生成一个帐户登录事件。此外，在用户登录而检索登录脚本和策略时，使用域帐户的成员服务器或工作站的交互式登录将在域控制器上生成登录事件。

如果定义该策略设置，可以指定是否审核成功、审核失败，或根本不对事件类型进行审核。登录成功时，成功审核会生成审核项。登录失败时，失败审核会生成审核项。

（5）审核对象访问

审核对象访问设置确定是否审核用户访问某个对象的事件，例如文件、文件夹、注册表项、打印机等，它们都有自己特定的系统访问控制列表（SACL）。

如果定义该策略设置，可以指定是否审核成功、审核失败，或根本不对该事件类型进行审核。当用户成功访问指定了合适 SACL 的对象时，成功审核将生成审核项。当用户访问指定有 SACL 的对象失败时，失败审核会生成审核项。

（6）审核策略更改

审核策略更改设置确定是否审核用户权限分配策略、审核策略或信任策略更改的每一个事件。

如果定义该策略设置，可以指定是否审核成功、审核失败，或根本不对该事件类型进行审核。对用户权限分配策略、审核策略或信任策略所作更改成功时，成功审核会生成审核项。对用户权限分配策略、审核策略或信任策略所作更改失败时，失败审核会生成审核项。



（7）审核特权使用

审核特权使用设置确定是否审核用户实施其用户权利的每一个实例。

如果定义该策略设置，可以指定是否审核成功、审核失败，或根本不对这种事件类型进行审核。用户权利实施成功时，成功审核会生成审核项。用户权利实施失败时，失败审核会生成审核项。

（8）审核过程跟踪

审核过程跟踪设置确定是否审核事件（例如程序激活、进程退出、句柄复制和间接对象访问等）的详细跟踪信息。

如果定义该策略设置，可以指定是否审核成功、审核失败，或根本不对该事件类型进行审核。所跟踪的过程成功时，成功审核会生成审核项。所跟踪的过程失败时，失败审核会生成审核项。

（9）审核系统事件

当用户重新启动或关闭计算机时或者对系统安全或安全日志有影响的事件发生时，安全设置确定是否予以审核。

如果定义该策略设置，可以指定是否审核成功、审核失败，或根本不对该事件类型进行审核。系统事件执行成功时，成功审核会生成审核项。系统事件执行失败时，失败审核会生成审核项。

13.1.2　设置审核策略

早期版本的 Windows 的审核策略是平级的，控制程度远不及现在的审核机制。在 Windows Vista 和 Windows Server 2008 中，审核策略是分层的，这是审核策略的一个重要的改变。

1. 审核策略简介

在 Windows Vista 和 Windows Server 2008 系统中，管理员可以使用两种工具设置审核策略：本地安全策略编辑器（在域环境中则可以使用组策略编辑器）和 AuditPol.exe 命令行工具。只有 AuditPol.exe 命令行工具能够在子类别级别设置审核策略：微软并没有将审核策略图形用户界面升级，如图 13.2 所示是 Windows Server 2008 审核策略配置的组策略机制包含审核策略子类别。

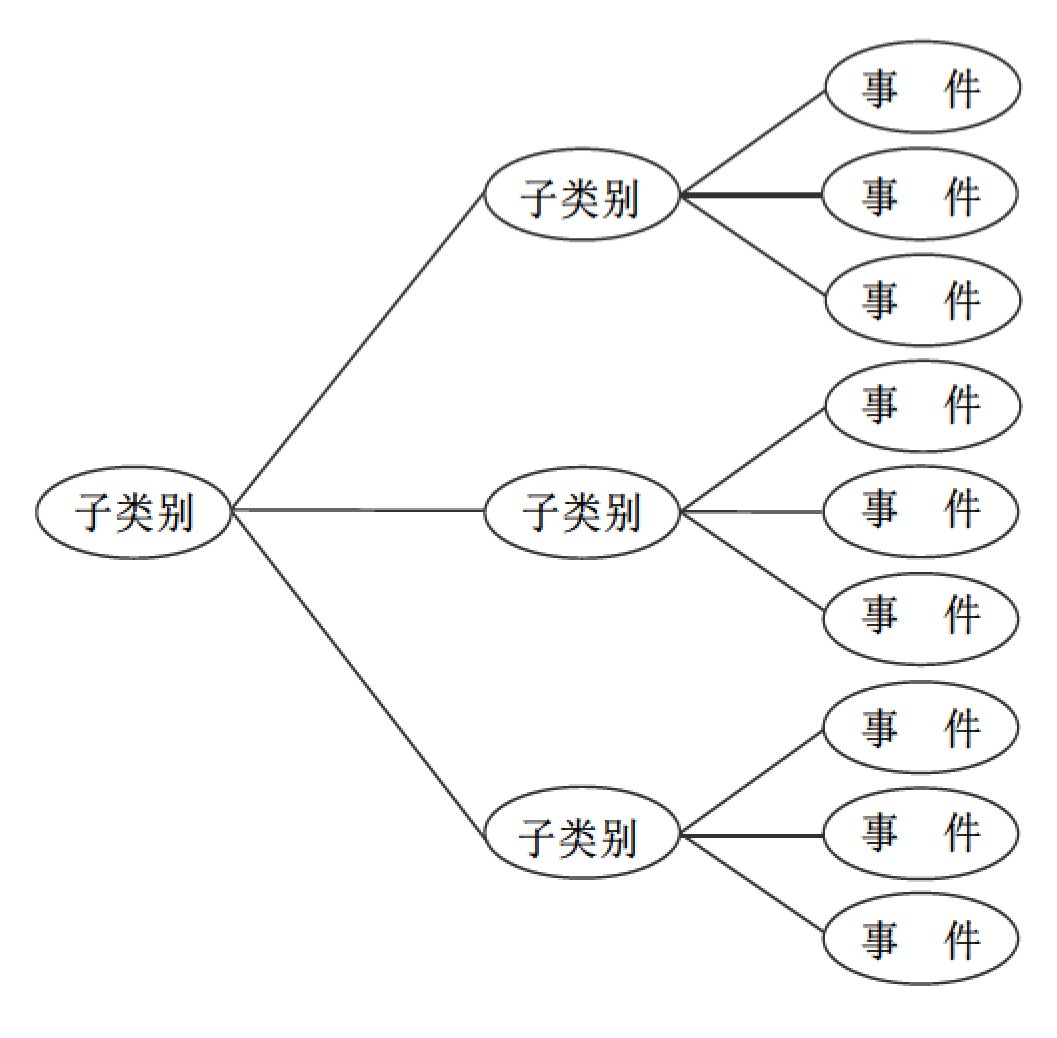


图 13.2　Windows Server 2008 的层级审核策略组织形式

审核策略的关键在于控制哪些事件生成并存储在审核日志中，新的 GAP（Generic

Access Profile，通用访问应用）特性是控制程度更高。大多数 Windows 系统是通过组策略从域中得到审核策略的（如图 13.3 所示），并不支持 GAP。这也说明可以为 Windows Server 2008 生成一个单独的审核策略，一旦将服务器与域联合，新的审核策略就将被组策略中传统的审核策略所覆盖。

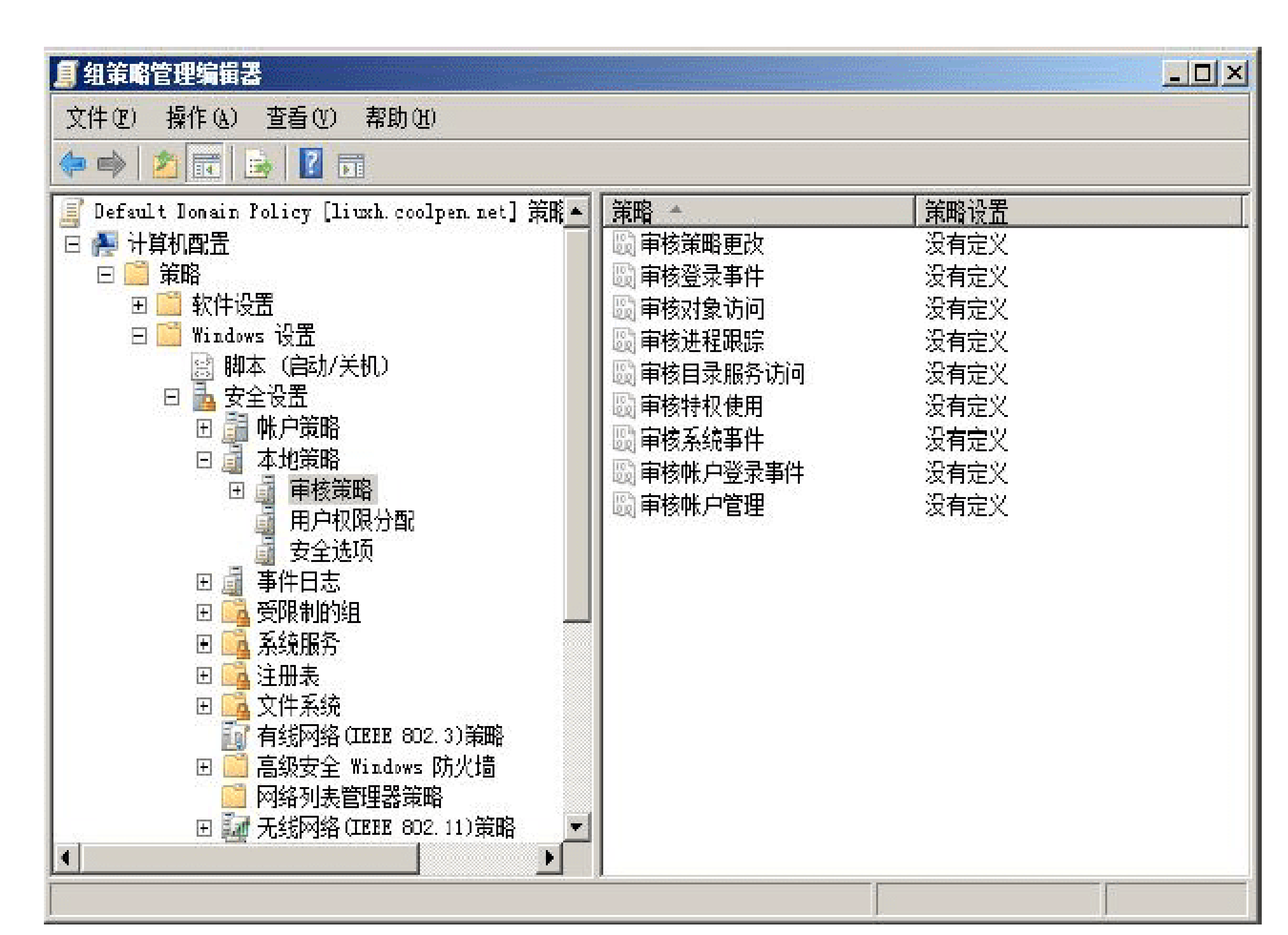


图 13.3　本地安全策略 MMC 快照中的审核策略用户界面

Microsoft 提供了一种机制，防止组策略分配的合法审核策略被 GAP 覆盖。一个名为 SCENoConfig LegacyAuditPolicy 的注册表值使得安全配置引擎（执行有关安全组策略设置的组件）应用于传统审核策略。如果将此注册表值设置为非零值，如果一级审核策略是通过安全策略快照或组策略设置的，就不适用了。

审核策略用户界面的另一局限性在于一级类别与子类别之间的关系。当用户使用 UI 来检测审核策略类别设置时，如果启用某类别的所有子类别，UI 就会显示启用该类别。同样的，如果所有相关子类别都禁用，UI 也会显示该类别是禁用的。但 UI 还用于另一种情况中——子类别中也有禁用和启用的。在这种情况下 UI 显示该类别为禁用，但用户可以通过 AuditPol.exe 程序查看正确有效的审核策略设置，如图 13.4 所示。



图 13.4　使用 AuditPol.exe 显示有效的 GAP 设置

该机制已通过验证并运行良好。如果需要改变审核策略设置，而却没有必要改变组策略对象（GPO）或脚本，用户就可以使用此方式来配置。这是通过使策略应用程序脚本在文本文件中阅读审核设置而实现的。

2. 审核策略选项

使用 AuditPol.exe 或本地或组策略模式中的安全策略时，在用户界面的安全选项中可以启用一些与审核策略相关的功能。

单一级别的操作系统中，如果无法记录安全审核，立即关闭系统（CrashOnAuditFail）设置通用准则需求，以保护文件。通用准则需求指的是，当审核系统无法生成或是存储日志时，系统必须暂停所有的审核活动。在 Windows 中，当审核系统不能安全记录时，是通过暂停系统（以蓝屏形式）来停止其活动的。在出现“CrashOnAuditFail”后，系统重启后只有管理员可以登录，直到安全事件日志被清除，导致错误的情况恢复正常后，其他用户才可以登录。只



有必要时，才能使用此设置，其可能会导致拒绝服务攻击。

出现 CrashOnAuditFail 有 3 种情形：

- 特性不能启用；
- 启用特性，但系统并没有出现问题；
- 启用特性，由于审核系统错误出现了问题，并且系统已重启。在这种情况下只有系统管理员可以登录。直到将 CrashOnAuditFail 设置为禁止或允许并且清除了日志后，普通用户方可登录。

完全特权审核（FullPrivilegeAuditing）设置会导致权限使用事件，若通过审核策略启用，其会授予除生成安全审核（SeAuditPrivilege）外的所有特权。在一般情况下，以下权限不生成特权使用事件：

- 跳过遍历检查（SeChangeNotifyPrivilege）；
- 调试程序（SeDebugPrivilege）；
- 创建令牌对象（SeCreateTokenPrivilege）；
- 替换进程级令牌（SeAssignPrimaryTokenPrivilege）；
- 生成安全审核（SeAuditPrivilege）；
- 备份文件和目录（SeBackupPrivilege）；
- 还原文件和目录（SeRestorePrivilege）。

禁止这些权限的主要原因，是由于普通操作系统和应用程序频繁使用这些权限，或在备份和还原权限的情况下，会导致容量过大。此外，如果生成审核权限的作用是其自身审核，日志就会填满此事件，因此从不审核 SeAuditPrivilege。概括地讲，安全事件日志中的所有事件，都是 SeAuditPrivilege 的一个特权使用事件；但如果不需要，则不要启用。

审核全局系统对象（AuditBaseObjects）和审核全局系统目录（AuditBaseDirectories）设置会导致在创建命名核心对象（例如互斥和信号量）时，为其添加 SACL。AuditBaseDirectories 影响容器对象，AuditBaseObjects 影响无法容纳其他对象的对象。基础对象用于同步进程。大多数核心对象是非命名的，使用句柄来表示。进程的句柄是唯一的，无法查看或访问未创建的非命名核心对象。命名核心对象是可见的，除非进程请求私有名称空间。使用命名核心对象时也有风险，如果不安全，则恶意进程可以操纵命名核心对象，导致系统出现问题。这种攻击手段叫做“蹲守攻击（squatting attack）”。使用 AuditBaseObjects 和 AuditBaseDirectories 可以审核这些对象的访问，从日志中检测蹲守攻击。

AuditBaseObjects 和 AuditBaseDirectories 的主要问题在于能够导致很大的审核容量，因为在基本操作中对这些对象的访问数量巨大。使用的 SACL 也是经过硬编码的，用户无法调整它们，但在 Windows Vista 和 Windows Server 2008 中不同，只有审核能够赋予访问这些对象的权限，这就大大减少了其容量。SACL 机制的另一限制在于，SACL 从系统启动创建对象时开始一直持续着整个进程运行的过程中，如果对象不毁灭，SACL 就不会改变，通常在创建该对象的进程终止或关闭时，对象就被毁灭了（对于系统对象来说）。要使启用或禁用 AuditBaseObjects 或 AuditBaseDirectories 生效，就必须重新启动计算机。

有关核心对象的信息并没有中央存储。多数软件开发机构不会公开此类信息，因为这涉及

到软件的内部运行方式，并且用户不能对其进行设置。所以，即使启用 AuditBaseObjects 或 AuditBaseDirectories，也很难确定一个对象的作用，除非该对象的名称是描述性的。因此，在研发环境中最好不要允许此类设置。用户可以使用微软工具程序集网站（http://www.microsoft.com/technet/sysinternals/SystemInformation/ProcessExplorer.mspx）上的进程管理器工具来检测基础对象（如图 13.5 所示）。

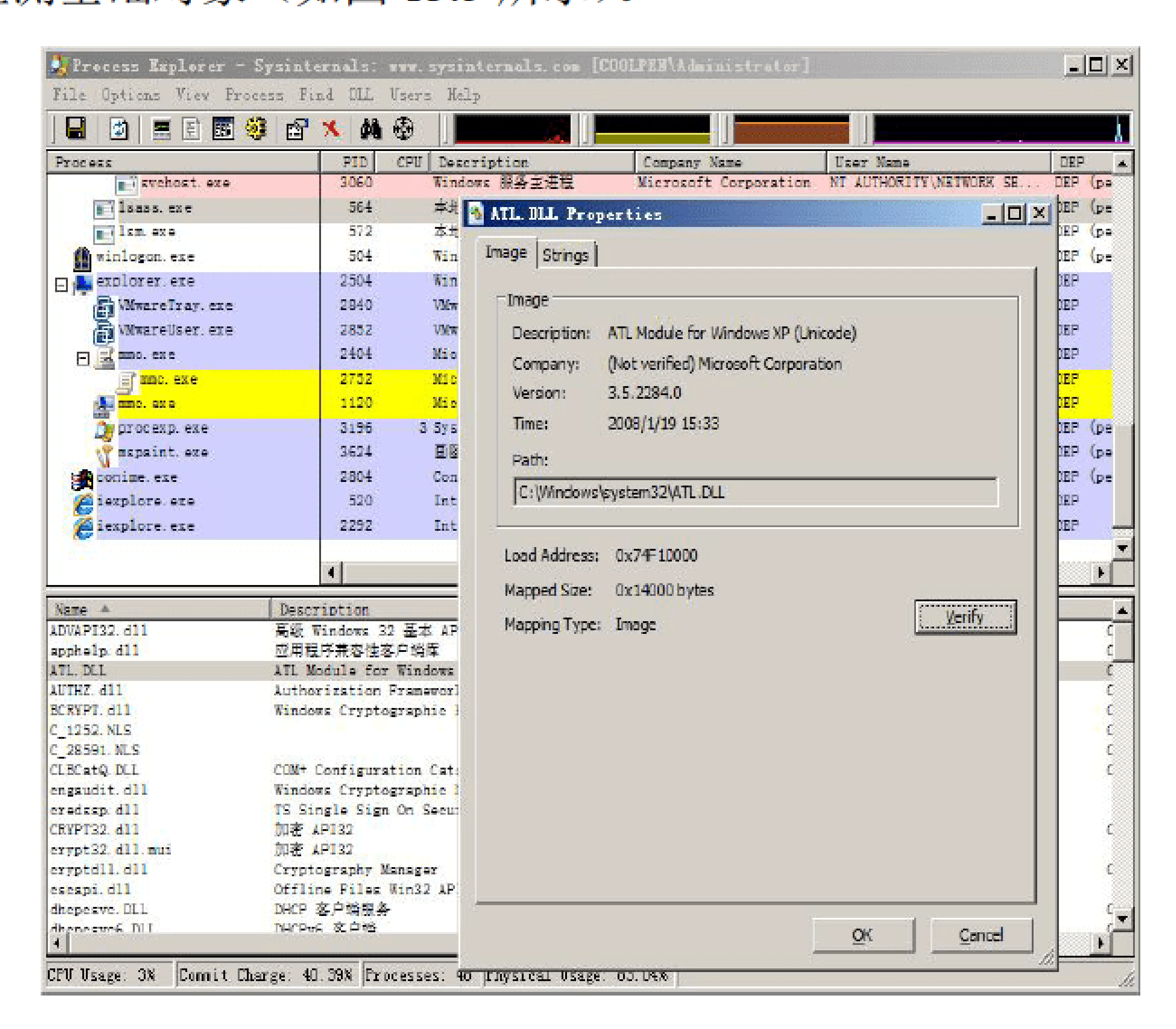


图 13.5　使用进程管理器检测对象

13.1.3　启用审核策略

Windows 系统可以提供 9 类事件审核策略，对于每一类都可以指明是审核成功事件、失败事件，还是两者都审核。Windows Server 2008 系统启动了大部分本地审核策略，安全性更高，管理员可以依次单击“开始”→“管理工具”→“本地安全策略”→“本地策略”→“审核策略”，打开 Windows 审核策略窗口，在这里即可根据需要启用或关闭安全审核策略，如图 13.6 所示。升级为域控制器的 Windows Server 2008 服务器，则需要在“组策略管理”控制台中完成。

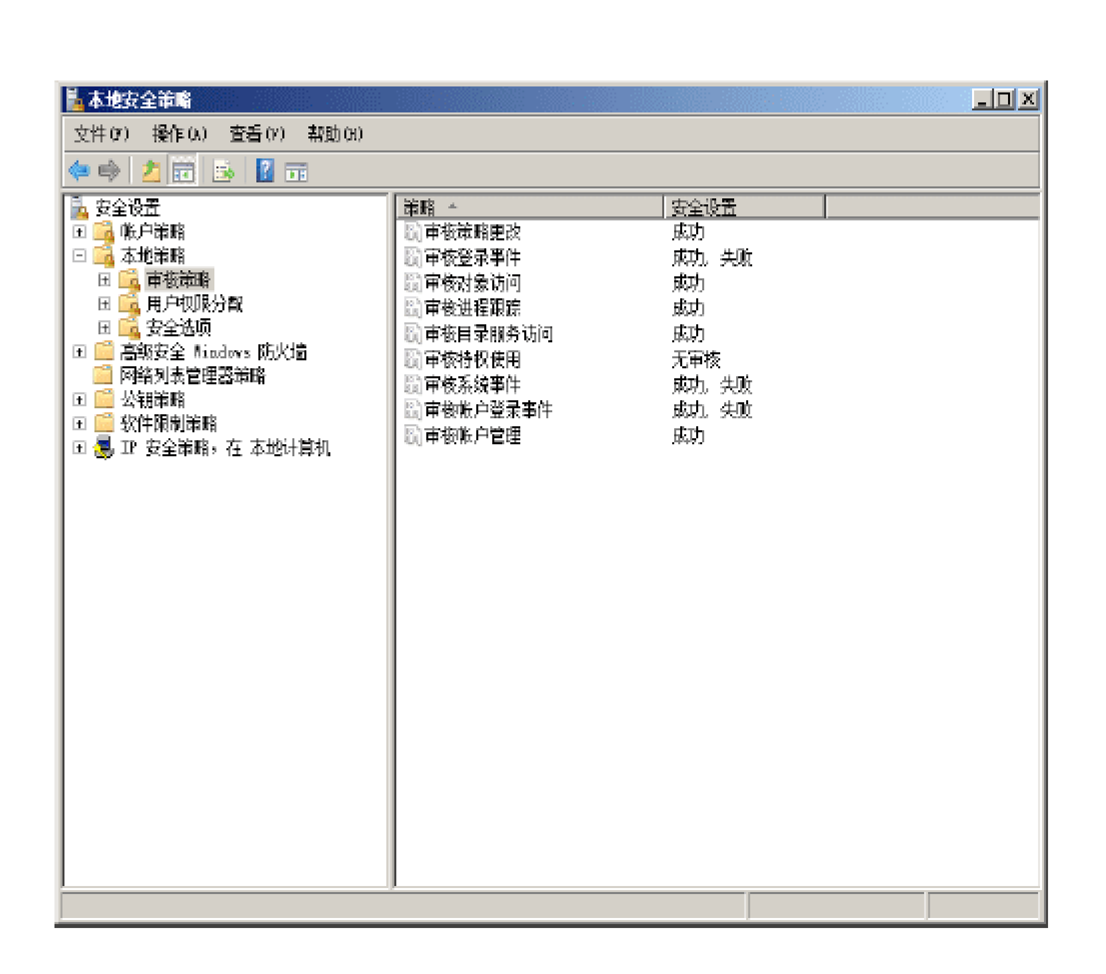


图 13.6　Windows 审核策略

Windows Server 2008 系统支持的事件审核策略包括：

- 审核策略更改：确定是否对用户权限分配策略、审核策略或信任策略做出更改的每一个事件进行审核。系统默认设置为“成功”，建议设置为“成功”和“失败”；
- 审核登录事件：确定是否审核用户登录到该计算机、从该计算机注销或建立与该计算机



网络连接的每一个实例。如果设定为审核“成功”，可用来确定哪个用户成功登录到哪台计算机；如果设为审核“失败”，可以用来检测入侵，但攻击者生成的庞大登录失败日志，会造成拒绝服务（DoS）状态。建议保持系统设置的“成功”状态；

- 审核对象访问：确定是否审核用户访问某个对象，例如文件、文件夹、注册表项、打印机等，它们都指定了自己的系统访问控制列表（SACL）的事件。建议设置为“失败”；
- 审核进程跟踪：确定是否审核事件的详细跟踪信息，例如程序激活、进程退出、间接对象访问等。如果怀疑系统被攻击，可启用该项，系统默认设置为“成功”；
- 审核目录服务访问：确定是否审核用户访问那些指定有自己的系统访问控制列表（SACL）的 Active Directory 对象的事件。启用后会在域控制器的安全日志中生成大量审核项，因此只有在确实要使用所创建的信息时才应启用。系统默认设置为“成功”；
- 审核特权使用：确定是否对用户行使用户权限的每个实例进行审核，但除跳过遍历检查、调试程序、创建标记对象、替换进程级别标记、生成安全审核、备份文件和目录、还原文件和目录等权限。系统默认为“无审核”；
- 审核系统事件：用于确定当用户重新启动或关闭计算机时，或者对系统安全或安全日志有影响的事件发生时，是否予以审核。这些事件信息是非常重要的，所以建议设置为“成功”和“失败”；
- 审核帐户登录事件：用于确定当用户登录到其他计算机（该计算机用于验证其他计算机中的帐户）或从中注销时，是否进行审核。建议设置为“成功”和“失败”；
- 审核帐户管理：用于确定是否对计算机上的每个帐户管理事件，如重命名、禁用或启用用户帐户、创建、修改或删除用户帐户或管理事件进行审核。建议设置为“成功”和“失败”。

Windows Server 2008 本地系统审核策略的配制方法，可参考本书“第 7 章　Windows 组策略”中的相关介绍。审核项目应配置得当，如果审核项目过多，不仅会影响服务器的响应速度，而且还会产生大量的日志文件，加重管理员工作负担。如果审核项目不足，无法准确记录恶意入侵和攻击情况，降低系统安全性。管理员可以在“事件查看器”中“Windows 日志”下的“安全”目录中查看产生的安全性日志。

13.1.4　审核事件 ID

事件 ID 是 Windows 事件的基本属性之一，在 Windows 事件查看器中，管理员可以根据系统为不同类型事件定义 ID 值，判断事件的类型和主要内容，筛选指定类型或 ID 的事件等。通过事件 ID 可以清楚地了解对服务器资源的非法访问和黑客的非法渗透。

1. 审核帐户登录事件

表 13.1 中列出了由“审核帐户登录事件”安全策略设置所生成的安全事件。

表 13.1　审核帐户登录事件

类别	事件 ID	内容
凭据验证类别	4774	使用被映射帐户进行登录
	4775	无法使用映射帐户进行登录
	4776	域控制器尝试验证凭据的帐户
	4777	域控制器无法验证凭据的帐户
Kerberos 身份验证服务类别	4768	请求 Kerberos 身份验证票证（TGT）
	4771	Kerberos 预身份验证失败
	4772	Kerberos 身份验证票证请求失败
Kerberos 服务票证操作类别	4769	Kerberos 服务票证请求
	4770	Kerberos 服务票证已续订

2. 审核帐户管理事件

表 13.2 中列出了由“审核帐户管理”安全策略设置所生成的安全事件。

表 13.2　审核帐户管理事件

类别	事件 ID	内容
应用程序组管理	4783	基本应用程序组已创建
	4784	基本应用程序组已更改
	4785	成员已添加到基本应用程序组
	4786	成员已从基本应用程序组删除
	4787	非成员已添加到基本应用程序组
	4788	成员被从基本应用程序组中删除
	4789	基本应用程序组已删除
	4790	已创建 LDAP 查询组
计算机帐户管理	4742	计算机帐户已更改
	4743	计算机帐户被删除
通讯组管理	4744	禁用安全的本地组已创建
	4745	禁用安全的本地组已更改
	4746	成员已被添加至禁用安全的本地组
	4747	成员已从禁用安全的本地组删除
	4748	禁用安全的本地组被删除
	4749	禁用安全的全局组已创建
	4750	禁用安全的全局组已更改
	4751	成员已添加至禁用安全的全局组
	4752	已从禁用安全的全局组删除成员
	4753	禁用安全的全局组已删除
	4759	禁用安全的通用组已创建
	4760	禁用安全的通用组已更改
	4761	成员已添加至禁用安全的通用组
	4762	已从禁用安全的通用组删除成员



（续表）

类别	事件 ID	内容
其他帐户管理事件	4739	更改域策略
	4782	访问帐户密码哈希
	4793	密码策略检查 API 调用程序
安全组管理	4727	安全启用全局组已创建
	4728	成员已添加至启用安全的全局组
	4729	从安全启用全局组已删除成员
	4730	安全启用全局组已删除
	4731	安全启用本地组已创建
	4732	成员已添加至启用安全的本地组
	4733	成员已从启用安全的本地组删除
	4734	安全启用本地组被删除
	4735	安全启用本地组已更改
	4737	安全启用全局组已更改
	4754	安全启用通用组已创建
	4755	安全启用通用组已更改
	4756	成员已添加至启用安全的通用组
	4757	成员已从启用安全的通用组删除
	4758	安全启用通用组已删除
	4764	组类型已更改
用户帐户管理	4720	创建用户帐户
	4722	用户帐户被启用
	4723	试图更改帐户的密码
	4724	试图重置帐户的密码
	4725	用户帐户被禁用
	4726	用户帐户被删除
	4738	用户帐户已更改
	4740	用户帐户被锁定
	4765	SID 历史添加到帐户
	4766	帐户添加 SID 历史的尝试失败
	4767	已锁定用户帐户
	4780	这是管理员组的成员帐户上设置 ACL
	4781	帐户的名称已更改
	4794	被试图设置目录服务还原模式
	5376	凭据管理器凭据被备份
	5377	凭据管理器凭据已从备份还原

3. 审核详细跟踪事件

表 13.3 中列出了由“审核详细跟踪”安全策略设置所生成的安全事件。

表 13.3 审核详细跟踪事件

类别	事件 ID	消息
DPAPI 活动	4692	尝试数据保护主密钥备份
	4693	尝试对数据保护主密钥恢复
	4694	尝试保护的审计保护数据
	4695	尝试未保护的审计保护数据
进程创建	4688	已创建一个新进程
	4696	主令牌被分配给处理
进程中止	4689	进程已退出
RPC 事件	5712	试图远程过程调用（RPC）

4. 审核目录服务访问事件

表 13.4 中列出了由“审核目录服务访问”安全策略设置所生成的安全事件。

表 13.4 审核目录服务访问事件

类别	事件 ID	消息
详细目录服务复制	4928	建立 Active Directory 副本源命名上下文
	4929	删除 Active Directory 副本源命名上下文
	4930	修改 Active Directory 副本源命名上下文
	4931	修改 Active Directory 副本目标命名上下文
	4934	复制 Active Directory 对象的属性
	4935	开始复制失败
	4936	结束复制失败
	4937	从副本延迟对象删除
目录服务访问	4662	对象上进行操作
目录服务更改	5136	修改目录服务对象
	5137	已创建目录服务对象
	5138	目录服务对象是未删除
	5139	移动目录服务对象
	5141	删除目录服务对象
目录服务复制	4932	Active Directory 命名上下文的副本同步已开始
	4933	Active Directory 命名上下文的副本同步已结束

5. 审核登录/注销事件

表 13.5 中列出了“审核登录/注销事件”安全策略设置所生成的安全事件。



表 13.5　审核登录/注销事件

类别	事件 ID	消息
帐户锁定	4625	帐户无法登录
IPSec 扩展模式	4978	在扩展模式协商，IPSec 收到一个无效协商数据包。 如果问题仍然存在， 则可能说明网络问题或者试图修改或重播该协商
	4979	已建立 IPSec 主模式和扩展模式安全关联
	4980	已建立 IPSec 主模式和扩展模式安全关联
	4981	已建立 IPSec 主模式和扩展模式安全关联
	4982	已建立 IPSec 主模式和扩展模式安全关联
	4983	IPSec 扩展模式协商失败，相应的主模式安全关联已被删除
	4984	IPSec 扩展模式协商失败，相应的主模式安全关联已被删除
IPSec 主模式	4646	IKE 预防 DoS 攻击模式启动
	4650	已建立 IPSec 主模式安全关联，没有启用扩展模式，不使用证书验证
	4651	已建立 IPSec 主模式安全关联，没有启用扩展模式，证书用于身份验证
	4652	IPSec 主模式协商失败
	4653	IPSec 主模式协商失败
	4655	IPSec 主模式安全关联结束
	4976	在主模式协商过程中，IPSec 收到一个无效协商数据包
	5049	删除了 IPSec 安全关联
	5453	由于未启动 IKE 和 IPSec Keying 模块服务，IPSec 协商与远程计算机失败
IPSec 快速模式	4654	IPSec 快速模式协商失败
	4977	在快速模式协商过程中，IPSec 收到一个无效协商数据包
	5451	已建立 IPSec 快速模式安全关联
	5452	IPSec 快速模式安全关联结束
注销	4634	帐户被注销
	4647	用户启动注销
登录	4624	已成功登录帐户
	4625	帐户无法登录
	4648	试图使用明确凭据登录
	4675	SID 被筛选
网络策略服务器	6272	网络策略服务器授予用户访问权限
	6273	网络策略服务器用拒绝户访问
	6274	网络策略服务器放弃对用户请求
	6275	网络策略服务器丢弃记帐请求的用户
	6276	网络策略服务器隔离一个用户
	6277	网络策略服务器授予用户访问，但因为主机不符合定义策略而被阻止

（续表）

类别	事件 ID	消息
网络策略服务器	6278	主机满足网络策略服务器定义的状况策略，授予完全访问
	6279	由于重复验证失败，网络策略服务器锁定用户帐户
	6280	网络策略服务器取消锁定用户帐户
其他登录/注销事件	4649	检测重播攻击
	4778	重新会话已连接到窗口站
	4779	从窗口站会话被中断
	4800	锁定工作站
	4801	是锁定工作站
	4802	屏幕保护程序被调用
	4803	已关闭屏幕保护程序
	5378	请求凭据委派是允许通过策略
	5632	对到无线网络进行了请求
	5633	对到有线网络进行了请求
特殊登录	4964	特殊组已分配给新登录

6. 审核对象访问事件

表 13.6 中列出了由“审核对象访问”安全策略设置所生成的安全事件。

表 13.6　审核对象访问事件

类别	事件 ID	消息
生成应用程序	4665	一个试图创建一个应用程序客户端上下文
	4666	应用程序尝试的操作
	4667	删除应用程序客户端上下文
	4668	初始化应用程序
证书服务	4868	证书管理员拒绝挂起证书请求
	4869	证书服务收到重复提交的证书请求
	4870	证书服务吊销证书
	4871	证书服务收到请求来发布证书吊销列表（CRL）
	4872	证书服务发行证书吊销列表（CRL）
	4873	更改证书申请扩展
	4874	一个或多个证书申请属性更改
	4875	证书服务接收到关闭请求
	4876	证书服务备份启动
	4877	证书服务备份完成
	4878	启动证书服务还原
	4879	证书服务还原完成
	4880	证书服务启动
	4881	证书服务停止



（续表）

类别	事件 ID	消息
证书服务	4882	对于证书服务安全权限更改
	4883	证书服务检索存档密钥
	4884	证书服务导证书入其数据库
	4885	对于证书服务审核筛选器更改
	4886	证书服务收到证书请求
	4887	证书服务批准证书申请并颁发证书
	4888	证书服务拒绝证书申请
	4889	证书服务设置到挂起证书请求的状态
	4890	证书管理设置对于证书服务更改
	4891	证书服务中更改一个配置项
	4892	更改属性的证书服务
	4893	证书服务存档了密钥
	4894	证书服务导入和存档密钥
	4895	证书服务 CA 证书发行到 Active Directory 域服务
	4896	已从证书数据库删除一个或多行
	4897	角色分离启用
	4898	证书服务加载模板
文件共享	5140	访问网络共享对象
文件系统子类别	4664	一个试图创建硬链接
	4985	事务的状态已更改
	5051	文件被虚拟化
筛选平台连接	5031	Windows 防火墙服务阻止应用程序接受传入连接在网络上
	5154	Windows 过滤平台具有允许应用程序或服务以端口上监听传入连接
	5155	Windows 过滤平台已阻止应用程序或服务从端口上监听传入连接
	5156	Windows 过滤平台具有允许建立连接
	5157	Windows 过滤平台已阻止建立连接
	5158	Windows 过滤平台具有允许绑定到本地端口
	5159	Windows 过滤平台已阻止绑定到本地端口
筛选平台数据包过滤	5152	Windows 过滤平台阻止数据包
	5153	限制性 Windows 过滤平台筛选已阻止数据包
句柄	4656	请求句柄对象
	4658	关闭该控点来关闭对象
	4690	被试图复制句柄到对象
其他对象访问事件	4671	应用程序试图通过 TBS 访问阻止序号
	4691	请求对一个对象间接访问
	4698	创建计划任务
	4699	删除计划任务
	4700	已启用计划任务
	4701	计划任务被禁用

（续表）

类别	事件 ID	消息
其他对象访问事件	4702	计划任务更新
	5888	修改 COM+目录中的对象
	5889	已从 COM+目录删除对象
	5890	对象被添加到 COM+目录
注册表	4657	修改注册表值
	5039	虚拟化注册表项
Multi-use 特殊子类别	4659	与意向来删除请求句柄对象
	4660	已删除对象
	4661	请求句柄对象
	4663	试图访问对象

7. 策略更改事件

表 13.7 中列出了由“策略更改”安全策略设置所生成的安全事件。

表 13.7　策略更改事件

类别	事件 ID	消息
审核策略更改	4715	更改对象上审核策略（SACL）
	4719	更改系统审核策略
	4902	创建用户审核策略表
	4904	被试图注册安全事件源
	4905	被试图注销安全事件源
	4906	CrashOnAuditFail 值已更改
	4907	更改审核设置对象上
	4908	修改特殊组登录表
	4912	每用户审核策略更改
验证策略更改	4706	新信任创建到域
	4707	删除对域信任
	4713	Kerberos 策略已更改
	4716	修改信任域信息
	4717	系统安全访问已授予帐户
	4718	从帐户删除系统安全访问
	4864	命名空间冲突检测
	4865	添加可信林中信息项
	4866	删除可信林中信息项
	4867	修改信任林信息项
授权策略更改	4704	分配用户右侧
	4705	右用户被删除
	4714	更改加密数据恢复策略



（续表）

类别	事件 ID	消息
筛选平台策略更改	4709	IPSec 服务已启动
	4710	IPSec 服务被禁用
	4711	可能包含下列之一： PAStore 引擎在计算机上应用 Active Directory 存储 IPSec 策略是本地缓存副本； PAStore 引擎在计算机上应用了 Active Directory 存储 IPSec 策略； PAStore 引擎在计算机上应用了本地注册表存储 IPSec 策略； PAStore 引擎无法在计算机上应用 Active Directory 存储 IPSec 策略副本； PAStore 引擎在计算机上应用 Active Directory 存储 IPSec 策略失败； PAStore 引擎在计算机上应用本地注册表存储 IPSec 策略失败； PAStore 引擎无法在计算机上应用某些规则的活动 IPSec 策略； PAStore 引擎无法加载目录存储 IPSec 策略在计算机上； PAStore 引擎加载目录存储 IPSec 策略在计算机上； PAStore 引擎无法加载本地存储 IPSec 策略在计算机上； PAStore 引擎加载本地存储 IPSec 策略在计算机上； PAStore 引擎轮询以了解对活动 IPSec 策略更改， 检测任何更改
	4712	IPSec 服务遇到可能严重错误
	5040	IPSec 设置已经更改。添加一个验证设置
	5041	IPSec 设置已经更改。验证设置了修改
	5042	IPSec 设置已经更改。验证设置一个被删除
	5043	IPSec 设置已经更改。添加连接安全规则
	5044	IPSec 设置已经更改。修改连接安全规则
	5045	IPSec 设置已经更改。删除连接安全规则
	5046	IPSec 设置已经更改。添加加密设置
	5047	IPSec 设置已经更改。加密设置被修改
	5048	IPSec 设置已经更改。加密设置被删除
	5440	下列标注为 Windows 筛选平台类别，在筛选引擎启动时显示
	5441	下列筛选器是 Windows 筛选平台类别，在筛选引擎启动时显示
	5442	下列提供程序是 Windows 筛选平台类别，在筛选引擎启动时显示
	5443	以下提供上下文是 Windows 筛选平台类别，在筛选引擎启动时显示
	5444	下列子层是 Windows 筛选平台类别，在筛选引擎启动时显示
	5446	Windows 过滤平台标注已更改
	5448	Windows 过滤平台提供程序已更改
	5449	Windows 过滤平台提供上下文已更改
	5450	Windows 过滤平台子层已更改
	5456	PAStore 引擎在计算机上应用了 Active Directory 存储 IPSec 策略
	5457	PAStore 引擎在计算机上应用 Active Directory 存储 IPSec 策略失败

（续表）

类别	事件 ID	消息
筛选平台策略更改	5458	PAStore 引擎在计算机上应用 Active Directory 存储 IPSec 策略是本地缓存副本
	5459	PAStore 引擎无法在计算机上应用 Active Directory 存储 IPSec 策略是本地缓存副本
	5460	PAStore 引擎在计算机上应用了本地注册表存储的 IPSec 策略
	5461	PAStore 引擎在计算机上应用本地注册表存储的 IPSec 策略失败
	5462	PAStore 引擎无法在计算机上应用某些规则的活动 IPSec 策略。使用 IP 安全监视器管理单元来诊断问题
	5463	PAStore 引擎轮询对活动 IPSec 策略更改，检测任何更改
	5464	PAStore 引擎轮询对活动 IPSec 策略更改， 检测更改， 并将其应用到 IPSec 服务
	5465	PAStore 引擎接收用于强制重新加载 IPSec 策略的控件和成功处理控件
	5466	PAStore 引擎对 Active Directory IPSec 策略进行轮询，Active Directory 无法使用 Active Directory IPSec 策略的缓存副本更改。无法应用上次轮询后对 Active Directory IPSec 策略的任何更改
	5467	PAStore 引擎对 Active Directory IPSec 策略进行轮询，Active Directory 可以获得所有策略更改。Active Directory IPSec 策略的缓存副本不再被使用
	5468	PAStore 引擎通过轮询了解 Active Directory IPSec 策略更改，确定 Active Directory 可被访问，找到对策略，并应用这些更改。Active Directory IPSec 策略的缓存副本不再被使用
	5471	PAStore 引擎加载本地存储 IPSec 策略在计算机上
	5472	PAStore 引擎无法加载本地存储 IPSec 策略在计算机上
	5473	PAStore 引擎加载目录存储 IPSec 策略在计算机上
	5474	PAStore 引擎无法加载目录存储 IPSec 策略在计算机上
	5477	PAStore 引擎无法添加快速模式筛选器
MPSSVC 规则 – 级别策略更改	4944	Windows 防火墙启动时下列策略处于活动
	4945	Windows 防火墙启动时被列出规则
	4946	Windows 防火墙例外列表已被进行更改，添加规则
	4947	Windows 防火墙例外列表已被进行更改，修改规则
	4948	Windows 防火墙例外列表已被进行更改，删除规则
	4949	Windows 防火墙设置已还原到默认值
	4950	Windows 防火墙设置已经更改
	4951	规则已忽略因为通过 Windows 防火墙无法识别其主版本号
	4952	由于通过 Windows 防火墙无法识别其次要版本号部分规则已被忽略，将强制规则的其他部分
	4953	因为无法解析规则，已忽略通过 Windows 防火墙
	4954	Windows 防火墙组策略设置已更改，已应用新设置



（续表）

类别	事件 ID	消息
MPSSVC 规则 – 级别策略更改	4956	Windows 防火墙已更改活动配置文件
	4957	Windows 防火墙未应用以下规则
	4958	由于规则引用此计算机上没有配置项目没有 Windows 防火墙采用以下规则
其他策略更改事件	4909	更改用于 TBS 本地策略设置
	4910	更改组策略设置 TBS
	5063	试图提供加密操作
	5064	试图加密上下文操作
	5065	试图加密上下文修改
	5066	试图加密函数操作
	5067	试图加密函数修改
	5068	试图为加密函数提供操作
	5069	试图加密函数属性
	5070	试图加密函数属性修改
	5447	Windows 过滤平台筛选已被更改
	6144	成功应用了组策略对象中安全策略
	6145	一个或多个处理安全策略组策略对象中时出错
Multi-use 特殊子类别	4670	更改对象上的权限

8. 审核特权使用事件

表 13.8 中列出了由“审核特权使用”安全策略设置所生成的安全事件。

表 13.8　审核特权使用事件

类别	事件 ID	内容
敏感特权使用 / 非敏感特权使用	4672	特殊权限赋予新登录
	4673	特权服务调用
	4674	试图在特权对象操作

9. 审核系统事件

表 13.9 中列出了由“审核系统事件”安全策略设置所生成的系统事件。

表 13.9　审核系统事件

类别	事件 ID	内容
IPSec 驱动程序	4960	IPSec 丢弃传入数据包完整性检查失败。如果问题仍然存在，则可能表明网络问题或该数据包被修改传输到此计算机中。验证从远程计算机发送数据包是否与由此计算机接收相同。此错误可能也表明其他 IPSec 实现互操作问题
	4961	IPSec 丢弃传入数据包重播检查失败。如果问题仍然存在，则可能表明本机重播攻击
	4962	IPSec 丢弃传入的数据包重播检查失败消息

（续表）

类别	事件 ID	内容
IPSec 驱动程序	4963	IPSec 丢弃应该已被保护的入站明文数据包。 这通常是由于到远程计算机更改其 IPSec 策略没有通知此计算机。这也可能是欺骗攻击尝试
	4965	IPSec 从远程计算机与一个正确安全参数索引(SPI)收到一个数据包。这通常由数据包被破坏，硬件故障。如果持续，这些错误验证从远程计算机发送数据包是否与由此计算机接收相同。此错误也可能表明其他 IPSec 实现互操作问题。这时，如果连接性是畅通的，这些事件可被忽略
	5478	IPSec 服务成功启动
	5479	IPSec 服务已成功关闭。关闭对 IPSec 服务可使计算机更危险的网络攻击或者将计算机暴露给潜在安全风险
	5480	IPSec 服务无法获取完整的计算机上网络接口列表。会因为某些网络接口的可能无法获得通过应用 IPSec 筛选器提供保护这带来潜在安全风险。使用 IP 安全监视器管理单元来诊断问题
	5483	IPSec 服务无法初始化 RPC 服务器。IPSec 服务无法启动
	5484	IPSec 服务遇到一个关键性失败，已关闭。关闭对 IPSec 服务可使计算机更危险的网络攻击或者将计算机暴露给潜在安全风险
	5485	IPSec 服务无法处理某些 IPSec 筛选器对即插即用事件对网络接口。会因为某些网络接口的可能无法获得通过应用 IPSec 筛选器提供保护这带来潜在安全风险。 使用 IP 安全监视器管理单元来诊断问题
其他系统事件	5024	Windows 防火墙服务成功启动
	5025	Windows 防火墙服务已停止
	5027	Windows 防火墙服务无法从本地存储器检索安全策略。服务将继续强制当前策略
	5028	Windows 防火墙服务无法分析新安全策略。服务将继续与当前实施策略
	5029	Windows 防火墙服务无法初始化驱动程序。服务将继续以强制当前策略
	5030	Windows 防火墙服务无法启动
	5032	Windows 防火墙无法通知用户它阻止应用程序接受传入连接在网络上
	5033	Windows 防火墙驱动程序成功启动
	5034	Windows 防火墙驱动程序已停止
	5035	Windows 防火墙驱动程序无法启动
	5037	Windows 防火墙驱动程序检测到关键运行错误。终止
	5058	密钥文件操作
	5059	密钥迁移操作
安全状态更改	4608	正在启动 Windows
	4609	关闭 Windows



（续表）

类别	事件 ID	内容
安全状态更改	4616	更改系统时间
	4621	管理员从审核失败状态恢复系统。用户不是管理员用户现在允许进行登录。某些审核活动可能没有已记录
安全系统扩展	4610	通过本地安全机构验证包被加载
	4611	已使用本地安全机构注册可信登录过程
	4614	通知包被加载安全帐户管理器
	4622	通过本地安全机构被加载安全程序包
	4697	系统中已安装服务
系统完整性	4612	已用内部资源分配给的审核消息队列通向丢失某些审核完
	4615	无效使用 LPC 端口
	4618	监视安全事件图案发生
	4816	RPC 检测解密传入消息时完整性冲突
	5038	代码完整性确定该图像的文件哈希无效。文件可能是因受到未经授权修改而损坏，或无效哈希运算错误
	5056	执行自检加密
	5057	加密基元操作失败
	5060	验证操作失败
	5061	加密操作
	5062	执行内核模式加密自检

13.1.5　优化审核策略

要保证审核有效进行，必须配置既能够生成用户需要的事件，又能够生成有助于管理最终日志的事件策略。如果没有正确设置审核策略，将可能导致生成大量事件。因此与其他安全策略一样，要通过要分析用户最关心的安全威胁，配置正确的策略来减小威胁，才会得到最有效的结果。

审核策略的许多设置看起来都很好，将其全部选择似乎没有什么不妥。然而，Windows 有可能会产生更多用户无法管理的审核，所以正确的选择能够减少安全威胁，并且简化审核的工作量。在选择了审核策略之后，推荐先在少数计算机上试用，以检查安全日志容量，如果容量比想象中的要大，就要考虑更换审核设置了。确认无误之后，再大规模部署。

在 Windows Server 2008 中系统中，管理员可以通过事件查看器检测是哪些策略设置引起的审核容量。事件查看器窗口允许用户使用任务类别（也就是子类别）、事件源、事件 ID 以及其他属性来将事件分组，并显示每组的总数，如图 13.7 所示。如果看到了一个大容量事件，可以多检查几个有关事件，以发现更多有用的信息。否则，就应考虑禁用生成该事件的策略。

选择了审核策略之后，经过了测试和转换后，就做好了配置的准备工作。

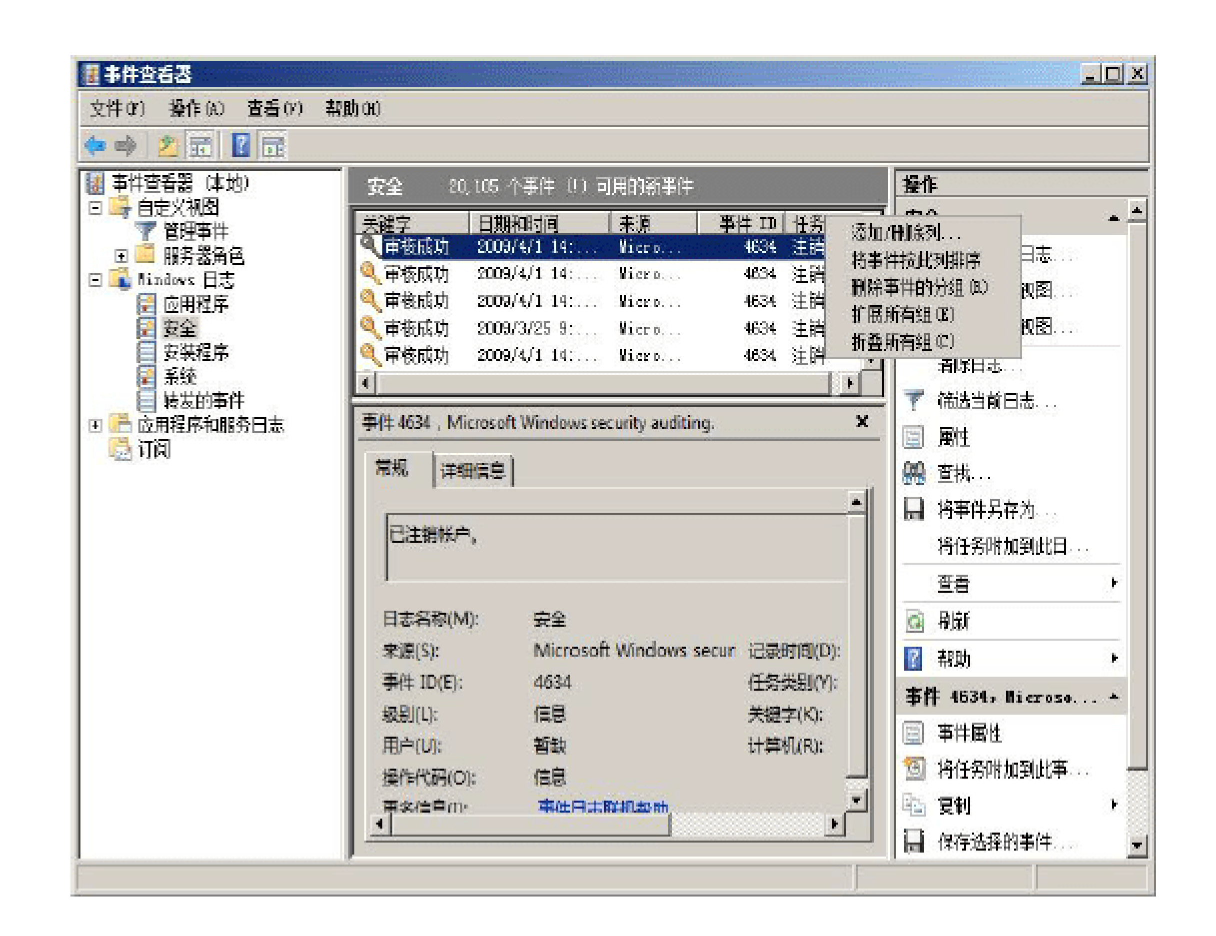


图 13.7　事件查看器通过任务类别将安全事件分组

13.2　系统事件和事件查看器

通常情况下，任何系统属性更改、运行状态的改变、应用程序的运行和停止，都会自动生成对应的系统事件日志。对于普通用户而言，可能很少关注这些细心，但对于服务器系统管理员而言，这些信息是非常重要的，直接决定服务器的稳定性、安全性和可靠性。在 Windows Server 2008 系统中，管理员可以通过事件查看器，查看、分析和解读系统事件日志，以便从中发现问题，及时制定解决问题的方案。

13.2.1　Windows Server 2008 安全事件新特点

与以前版本的 Windows 系统相比，Windows Server 2008 系统的安全事件日志进行了一些改进。最显著的变动就是事件 ID 号都被重新排序。Windows Serve 2008 中的安全事件的事件 ID 一般要比 Windows Server 2003 中的高 4096。例如登录成功事件，在 Windows Server 2003 中 ID 号为 528，在 Windows Server 2008 中为事件 4624（528+4096=4624）。另外，事件查看器中的事件属性信息内容有所变化。

Windows Server 2008 系统安全事件的改进主要表现在以下方面：

- 事件的布局安排发生了变化，使得定位要查找的信息更加方便了。并且出于显示目的将相似的信息分组；
- 多数事件添加了主题用来代替用户的作用。主题是指用于生成事件的帐户，也是执行审核活动的帐户。需要注意的是，这种情况下是本地系统，因为该活动不是“登录一个用户”，而是“登录一个用户帐户”。一个作为本地系统（WinLogon）运行的进程要求该登录。关于登录用户的信息，则会显示在另外的区域；
- 事件包含计算机友好相关区域和用户友好区域，例如，进程 ID（PID）与进程完整路径是在一起的；



- 事件查看器会显示两次用户帐户名，每个帐户的第一个例证都存储为安全标识符（SID），第二个例证存储为名称。事件查看器会自动将 SID 转译为帐户名。然而，由于名称是以明文的形式存储的，如果查看另一台未经备份或帐户已被删除的计算机的日志，仍可看到该名称（和转换的 SID）。在以前的版本中，名称查找错误是许多安全日志分析失败的原因；
- 增加了附加信息，如果以 NTLM 登录，就会列出与 NTLM 配套的协议（LM，NTLM V1，或 NTLM V2），如果已应用了 NTLMv2 会话密钥，就会列出密钥的长度。

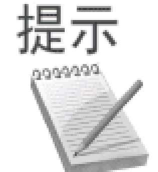
13.2.2　系统事件类型

Windows 操作系统中定义了 6 种事件类型，系统管理员可以根据关注的事件性质筛选希望查看的事件。表 13.10 显示了 Windows 系统定义的事件类型，及每个事件类型的具体含义。

表 13.10　事件类型及描述

事件类型	描述
错误	指明出现了问题，这可能会影响触发事件的应用程序或组件外部的功能。例如，如果在启动过程中某个服务加载失败，将会记录“错误”事件
警告	指明出现的问题可能会影响服务器或导致更严重的问题（如果未采取措施）。例如，当磁盘空间不足时，将会记录“警告”事件
信息	指明应用程序或组件发生了更改，如操作成功完成、已创建了资源，或已启动了服务
关键	指明出现了故障，导致触发事件的应用程序或组件可能无法自动恢复
Success Audit	指明出现了故障，导致触发事件的应用程序或组件可能无法自动恢复
审核失败	指明用户权限练习失败

提示



“Success Audit”和“审核失败”类型事件属于严重安全级别，可能出现在安全日志中。

13.2.3　事件查看器的应用

Windows 事件查看器的主要功能就是为管理员提供简洁、快速的时间浏览界面。Windows Server 2008 系统中新增了“自定义视图”和“应用程序和服务日志”功能，并且在“Windows 日志”中添加了“安装程序”和“转发的事件”查看功能，极大提高了网络管理员的工作效率。Windows Server 2008 系统的事件查看器，可以用来查看系统以及网络服务产生的日志记录信息，比 Windows Server 2003 事件查看器的功能强大了许多。

1. 查看事件信息

通过 Windows Server 2008 系统的事件查看器，可以管理服务器角色日志、Windows 系统日志和应用程序日志。事件日志中记录了事件发生的时间、事件来源、用户帐户、操作代码及了解详细相关信息的超级链接，管理员通过这些信息可以快速判断服务器或应用程序是否存在故障或安全隐患。在 Windows Server 2008 系统中，事件日志详细信息的基础结构完全符合 XML 架构，且可以访问代表给定事件的 XML。这也是 Windows Server 2008 区别于 Windows Server 2003 的主要方面之一。

01 打开“事件查看器”窗口，在左侧目录栏中展开希望查看和管理的事件日志类别，如“Windows 日志”→“安全”，如图 13.8 所示。系统默认已经启动“预览窗格”功能，即在事件列表中选择时间后，将自动显示相应预览信息。

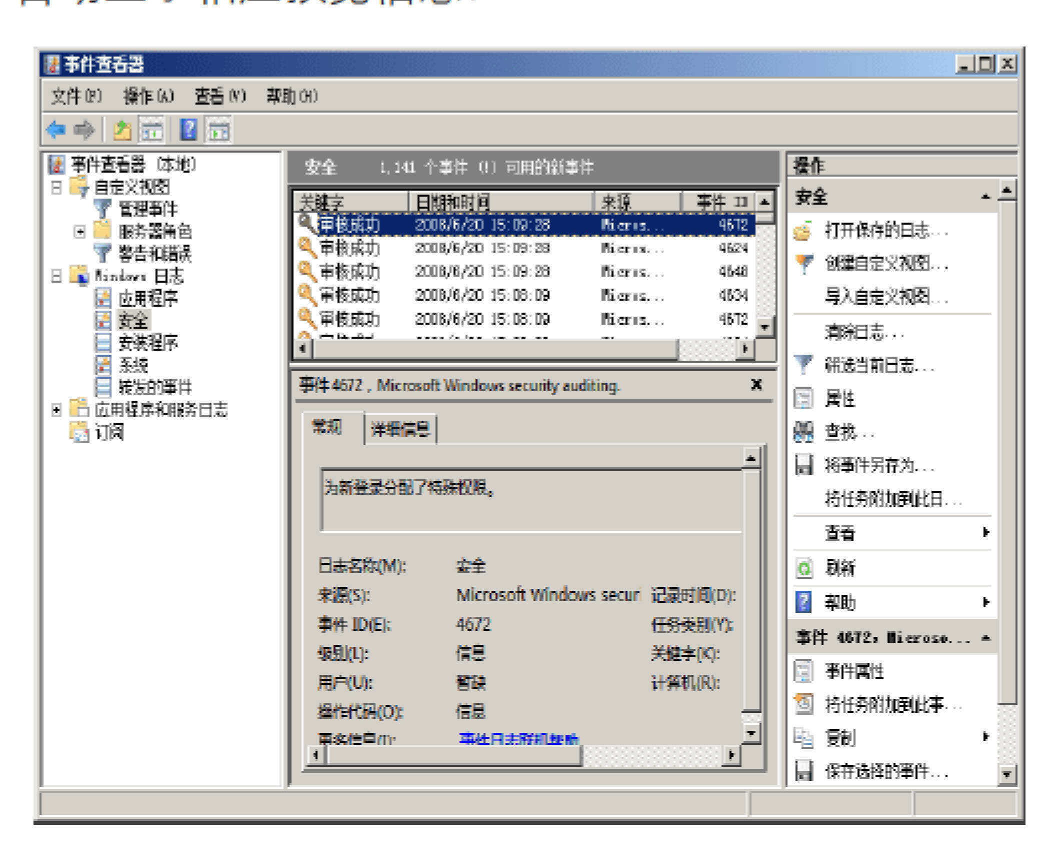


图 13.8 “事件查看器”窗口

02 双击其中的任何一个日志，便可查看详细信息。在日志属性窗口中，可以看到事件发生的日期，事件发生的源，事件发生的种类和 ID，以及事件的详细的描述，这些信息有助于帮助系统管理员解决安全问题。如图 13.9 所示是打开一个审核失败的安全事件。



图 13.9 “事件属性”对话框

03 单击“详细信息”切换至如图 13.10 所示“详细信息”选项卡，系统默认是以“友好视图”方式显示的。

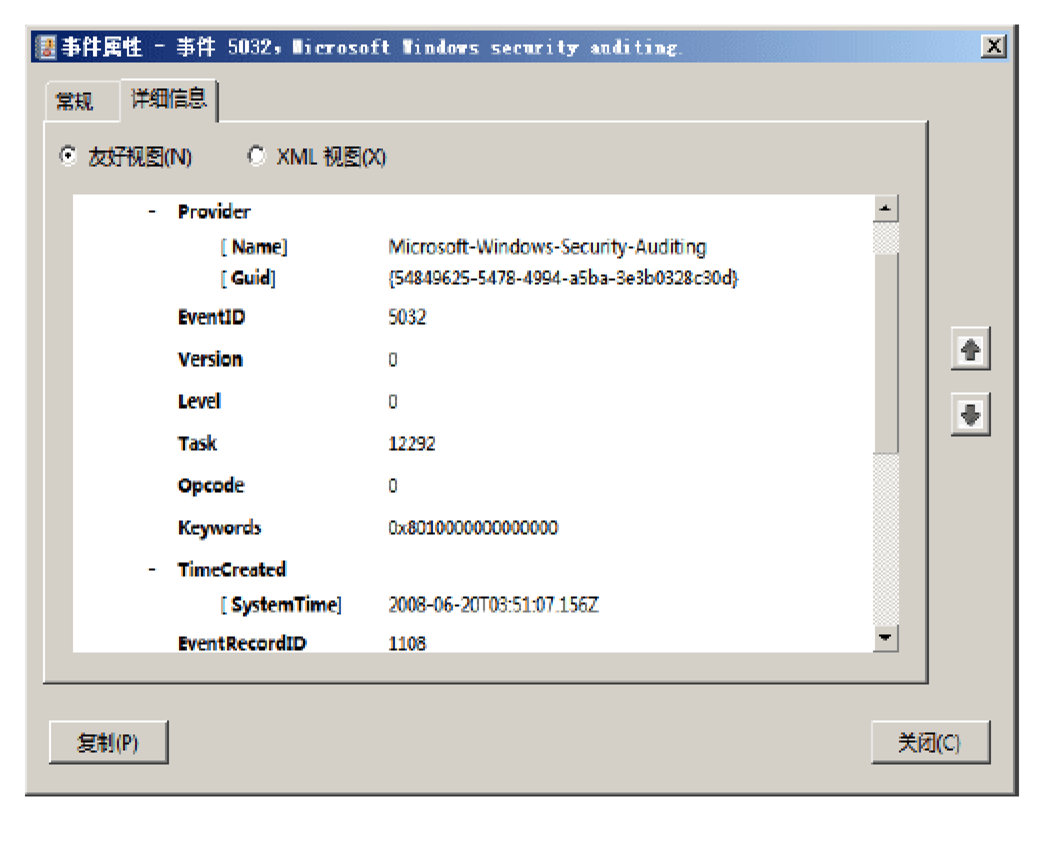


图 13.10 友好视图

04 选择“XML 视图”单选按钮，即可以 XML 视图方式显示事件详细信息，如图 13.11 所示。

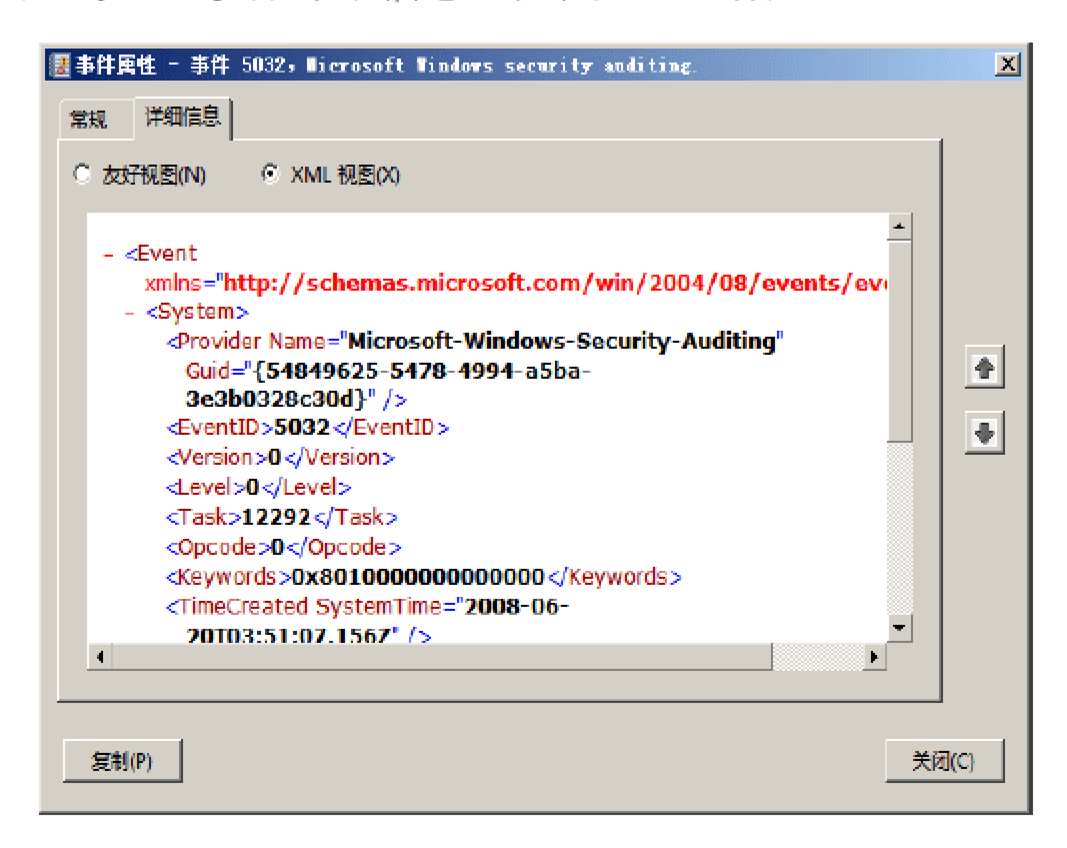


图 13.11 XML 视图

05 单击“关闭”按钮，关闭“事件属性”对话框即可。



2. 将任务附加到事件

Windows Server 2008 系统的事件查看器新增了通知、提醒功能，通过将计划任务附加到指定类型的事件，系统即可自动以某种方式通知用户，如发送 E-mail 邮件、弹出提示信息、开启程序等。可以选择一类系统事件作为关联对象，也可以选择单个事件进行关联。将任务附加到一类事件的具体操作步骤如下：

01 在“事件查看器”窗口中，右击“安装程序”（此处以“安装程序”类别的 Windows 事件为例），并选择快捷菜单中的“将任务附加到事件”，启动“创建基本任务向导”。依次单击“下一步”按钮，设置任务名称使用系统默认名称和操作类型，如图 13.12 所示。在“操作”对话框中，选择“发送电子邮件”单选按钮。

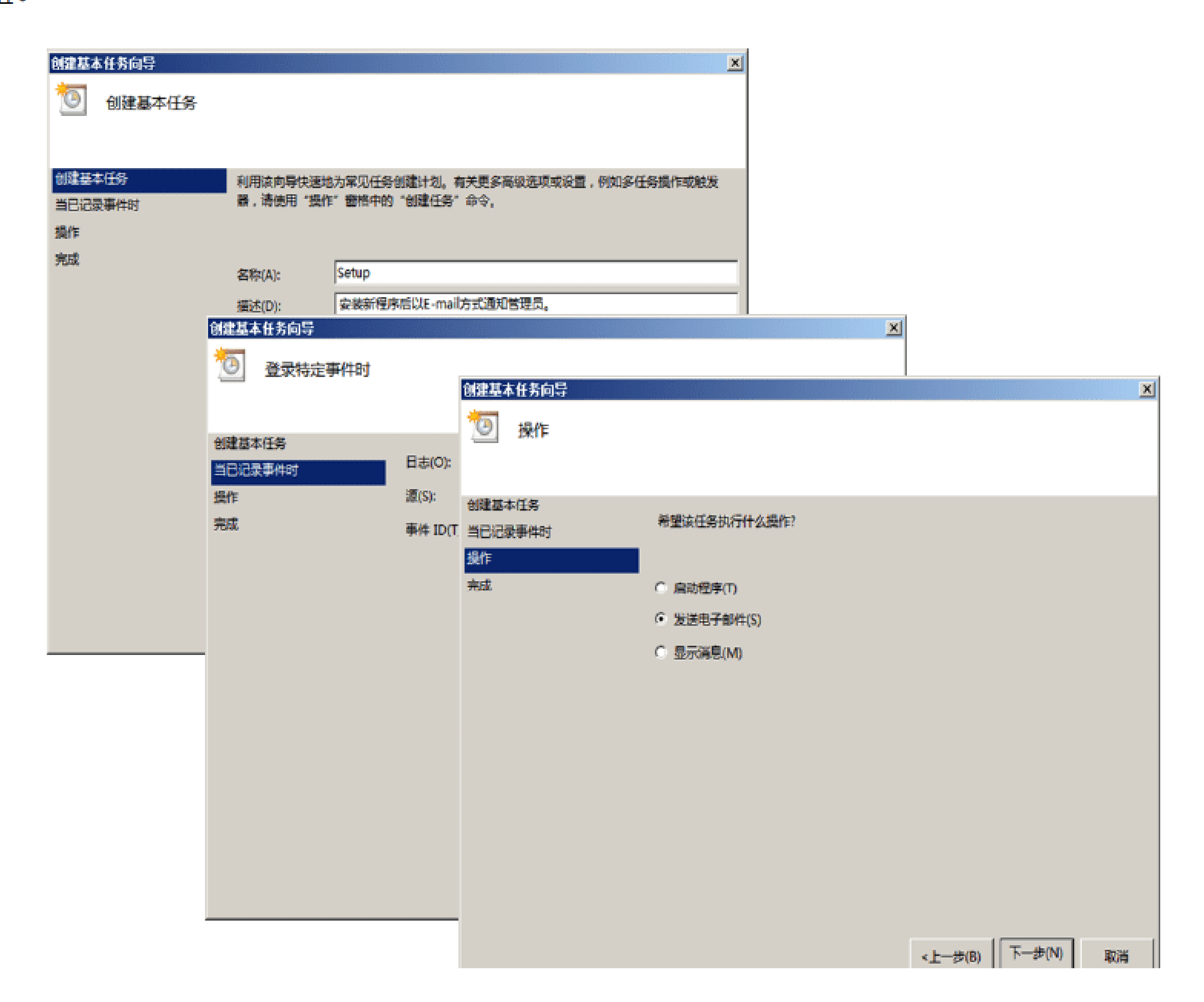


图 13.12　设置任务名称和操作类型

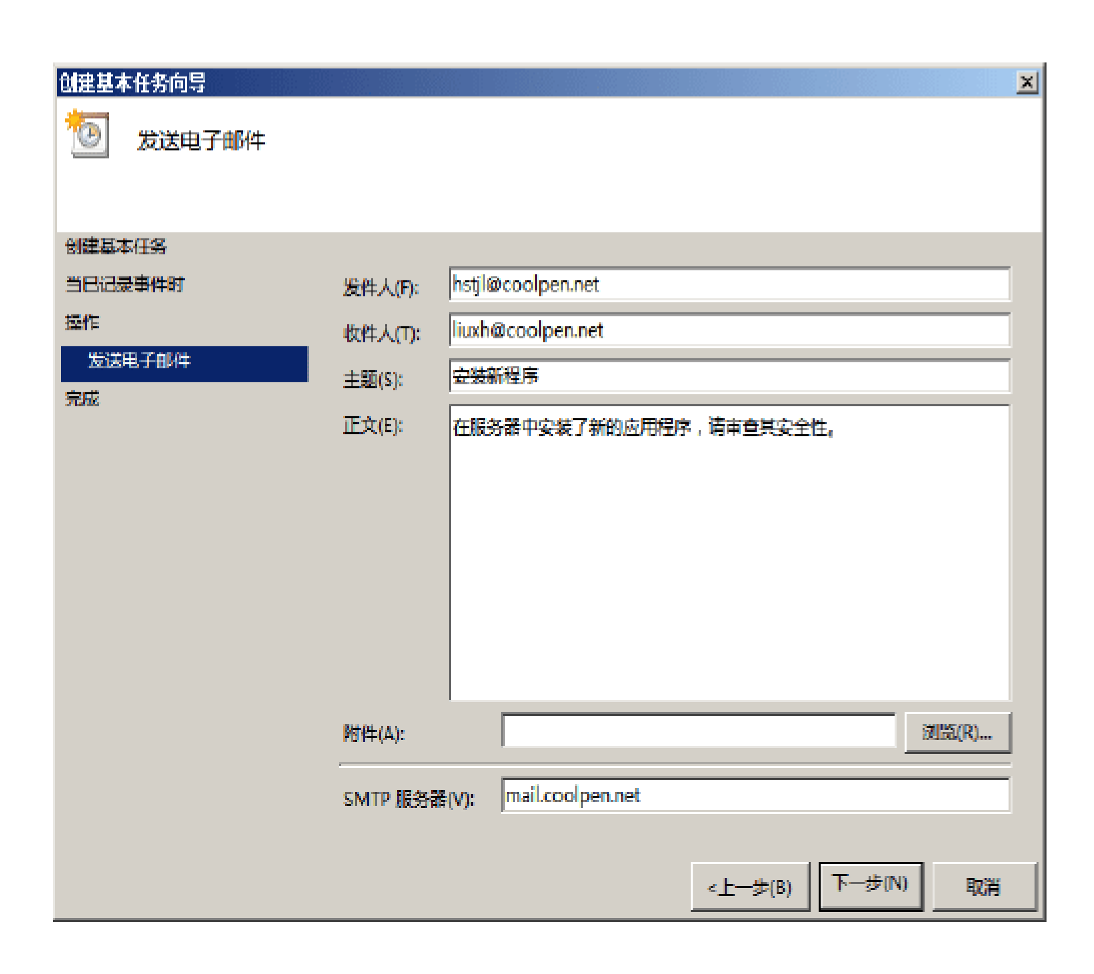


图 13.13　“发送电子邮件”对话框

02 单击“下一步”按钮，显示如图 13.13 所示“发送电子邮件”对话框。在“发件人”和“收件人”文本框中，输入希望使用的 E-mail 邮箱地址。在“正文”文本框中，可以输入简短的描述信息，告知用户发送此邮件的目的。

03 单击“下一步”按钮，显示如图 13.14 所示“摘要”对话框，提示当前已做的所有设置。如果选中“单击‘完成’时，打开此任务属性的对话框”复选框，关闭“创建基本任务向导”后，可以立即查看和编辑其属性设置。

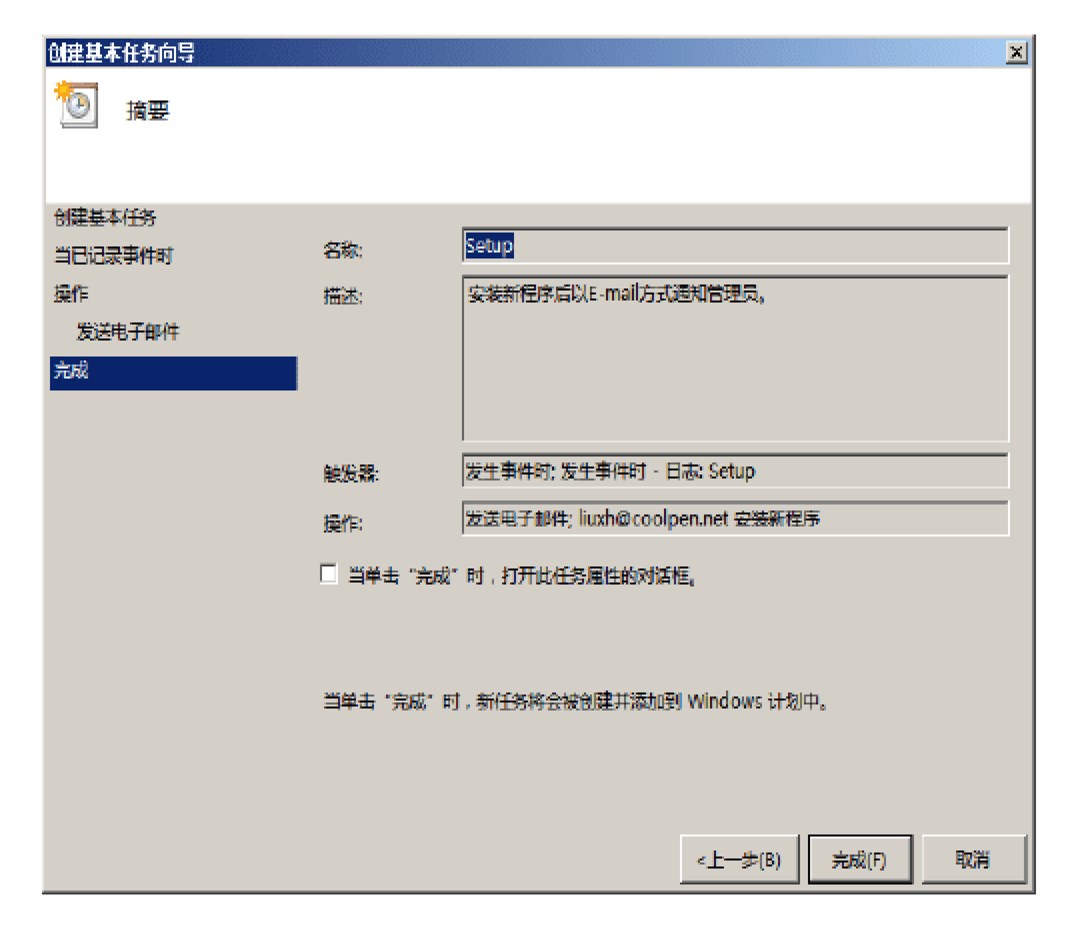


图 13.14 “摘要”对话框

04 单击“完成”按钮，打开如图 13.15 所示“事件查看器”提示框，提示计划任务已创建完成，可以在“任务计划程序”中查看和编辑计划的任务。

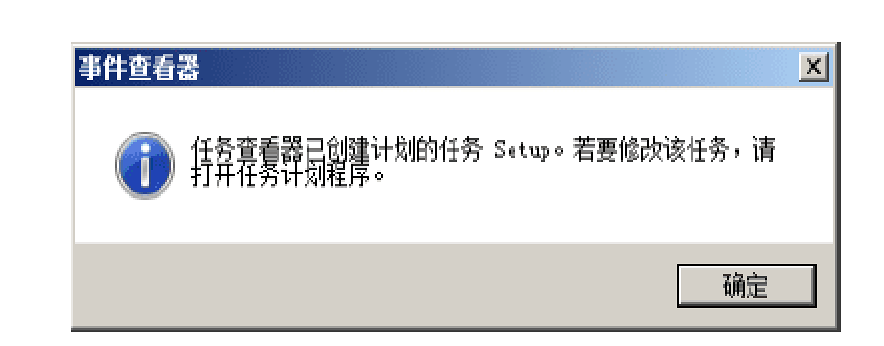


图 13.15 “事件查看器”提示框

05 单击“确定”按钮，关闭即可。



注意　在 Windows Server 2008 系统中，可以通过依次单击“开始”→“管理工具”→“任务计划程序”，打开“任务计划程序”窗口，在这里管理员可以对系统中所有的计划任务进行配置和管理。在“事件查看器”中创建的任务关联也会显示在这里，如图 13.16 所示。

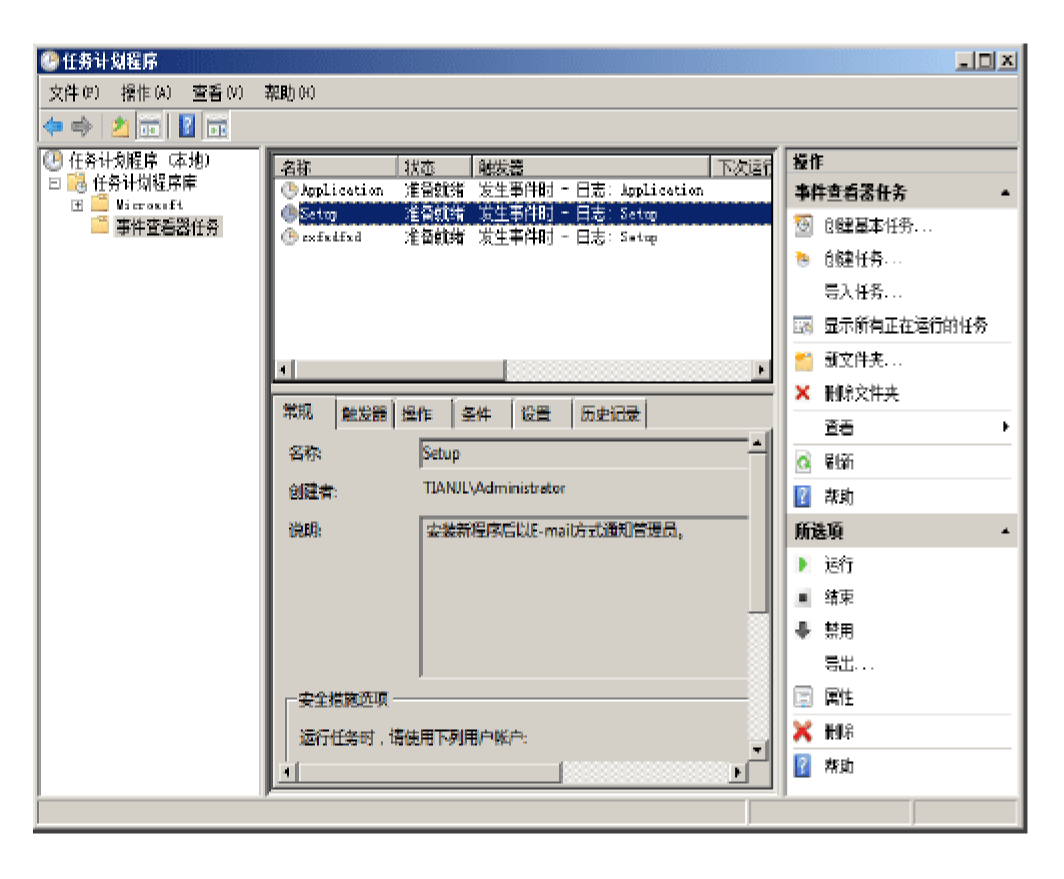


图 13.16 “任务计划程序”窗口

通过“创建基本任务向导”创建的任务关联计划，默认只能设置单一的“触发器（即执行任务的条件）”和“动作”。例如在“任务计划程序”窗口中，双击已创建的关联任务计划（以 setup 为例），打开“Setup 属性”对话框，在“操作”选项卡中，单击“新建”按钮，打开“新建操作”对话框，在“操作”下拉列表中，继续选择希望执行的操作类型即可，如图 13.17 所示。



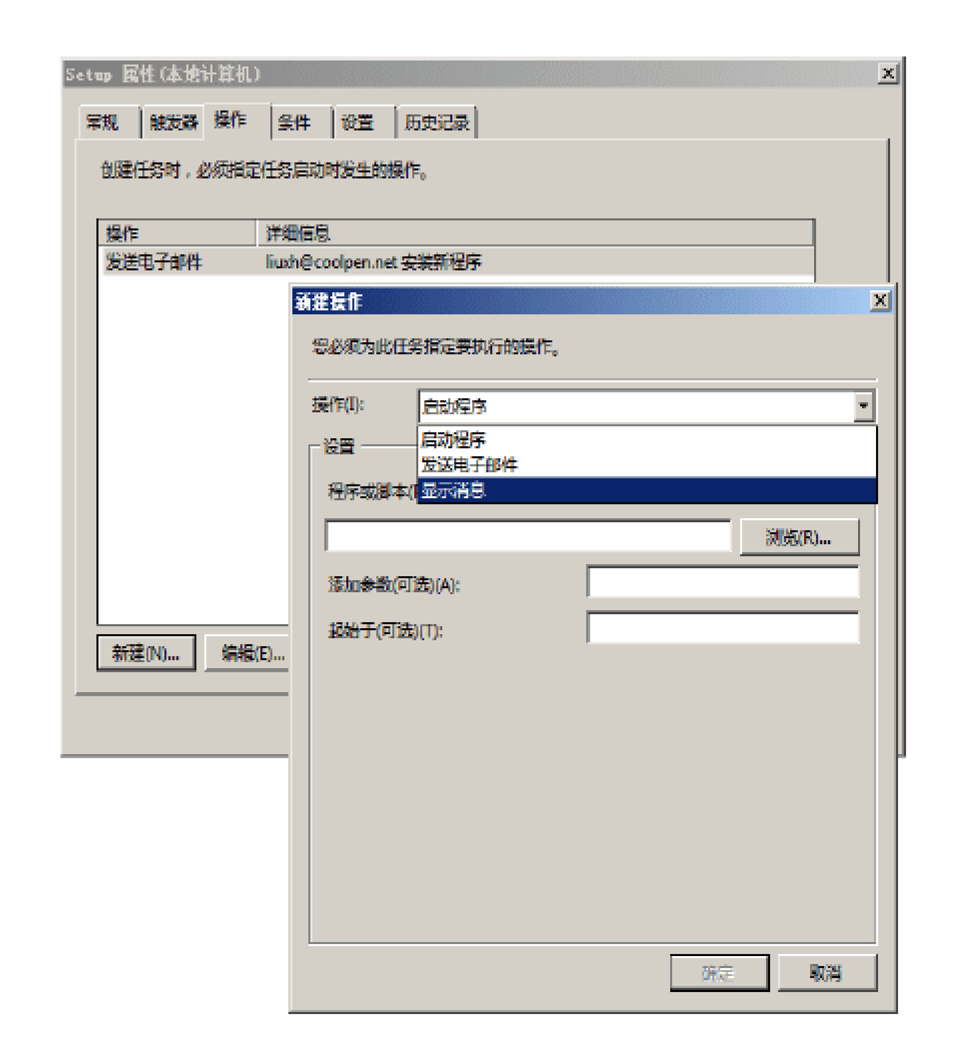


图 13.17　设置希望执行的操作

3. 导出和导入日志

如果 Windows 服务器的访问量非常大，每天产生的日志文件大小也是非常惊人的，尽管安装 Windows 系统和网络服务时，已经选择了安全可靠的日志保存目录，但为了确保日志文件的完整、安全，应适时将其备份至安全性较高的存储介质，如光盘或其他文件服务器等，以免由于系统故障或日志文件自动覆盖，而丢失重要信息。Windows Server 2008 系统中，导出日志文件的操作步骤如下（以 Windows 安全事件日志为例）：

01 在“事件查看器”窗口中展开“Windows 日志”，在导航栏中右击希望导出的时间类型，此处以“安全”事件为例，如图 13.18 所示。

02 选择快捷菜单中的“将事件另存为”，打开如图 13.19 所示“另存为”对话框。如果导出“自定义视图”中的服务器角色日志文件，需要选择快捷菜单中的“讲自定义视图中的事件另存为”。在“文件名”文本框中输入日志文件的名称，在“保存类型”下拉列表中，选择导出日志文件的格式，系统默认为*.evtx，此外还支持*.xml、*.txt 和*.csv 格式。其中只有*.evtx 日志文件，才可以在“事件查看器”中重新打开。如果把日志存档为文本（*.txt）或逗号分隔的格式（*.csv），可以在文字处理或电子表格之类的其他程序（而不是“事件查看器”）中重新打开日志，建议使用系统默认文件格式。

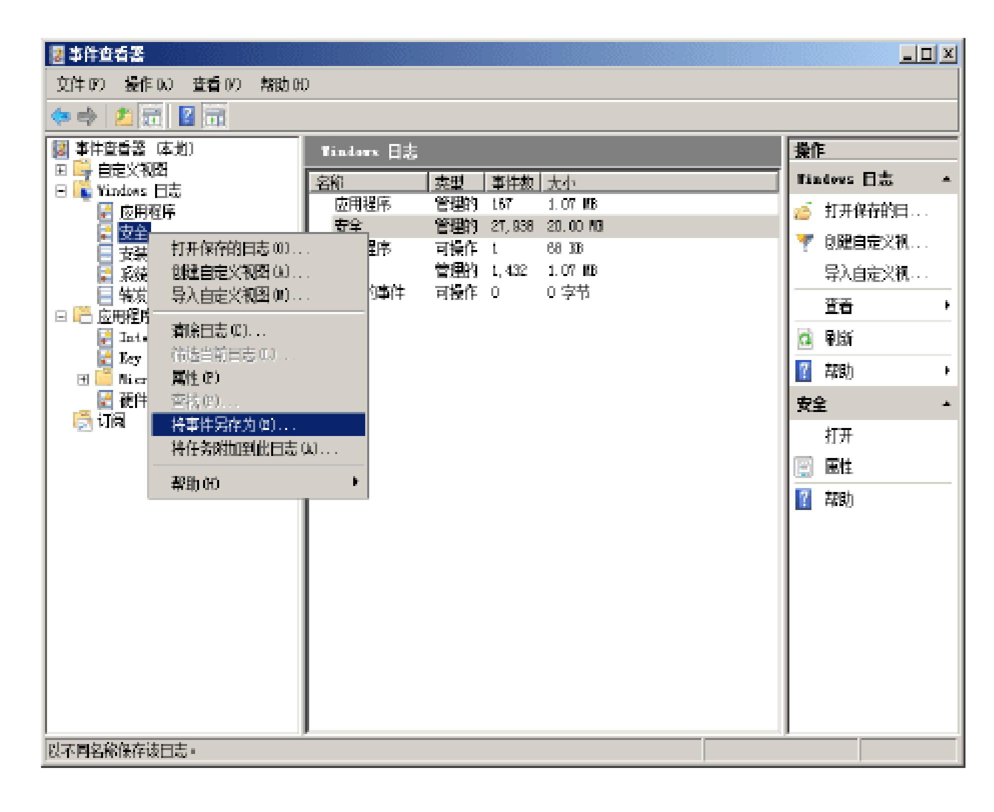


图 13.18　选择希望导出的事件类型

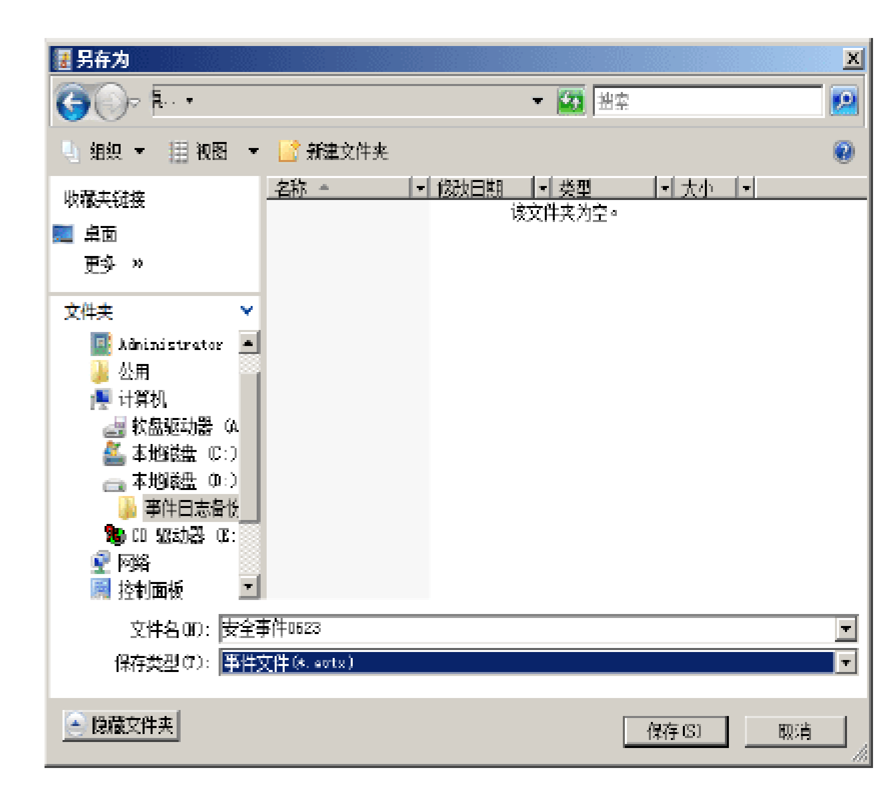


图 13.19　“另存为”对话框

提示 *.evtx是Windows Vista和Windows Server 2008系统的新文件格式，与早期Windows系统中的*.evt 文件相同。需要注意的是，*.evtx 文件只能在 Windows Vista 和 Windows Server 2008系统的“事件查看器”中打开。Windows Server 2008事件查看器可以兼容Windows Server 2003系统中导出的日志文件。

03 单击“保存”按钮，打开如图13.20所示“显示信息”对话框，系统默认选择“没有显示信息”单选按钮，此时导出日志只能在本地计算机或与本地计算机语言类型相同的其他计算机上打开。如果希望此日志可以在其他系统中查看，需要选择“显示这些语言的信息”单选按钮，并在列表框中选择与指定计算机系统匹配的语言类型。选中“显示所有可用的语言”复选框，即可显示当前系统支持的所有语言类型。

04 单击“确定”按钮，保存日志。

05 在其他计算机的“事件查看器”窗口中，右击导航栏中的任意项目，并选择快捷菜单中的“打开保存的日志”，打开如图13.21所示“打开保存的文件”对话框，选择希望导入的目标文件即可。

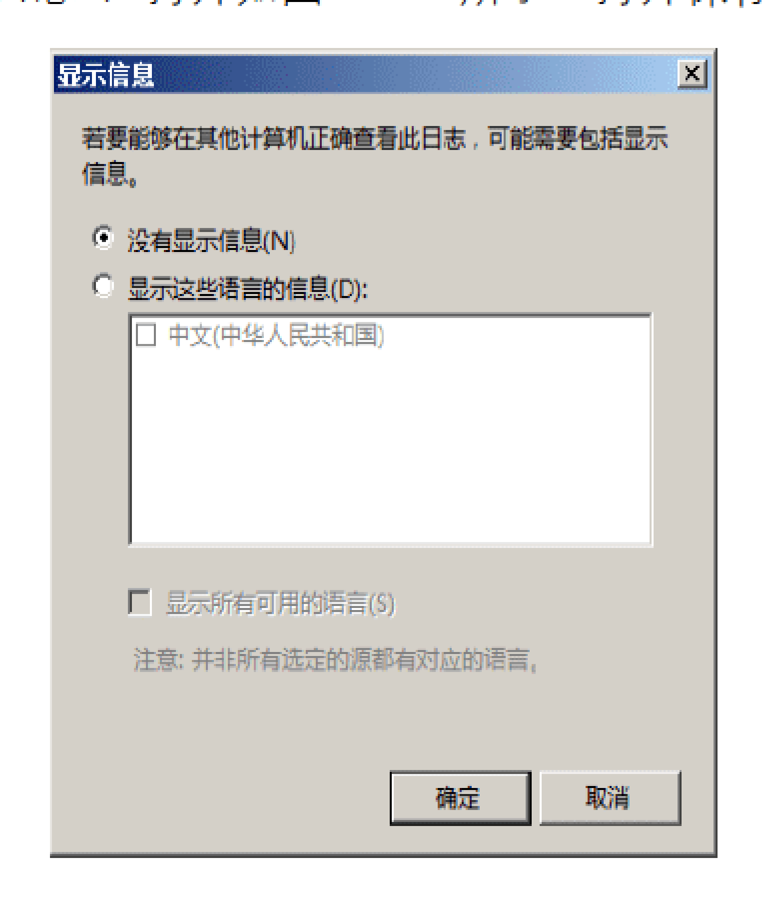


图13.20 “显示信息”对话框

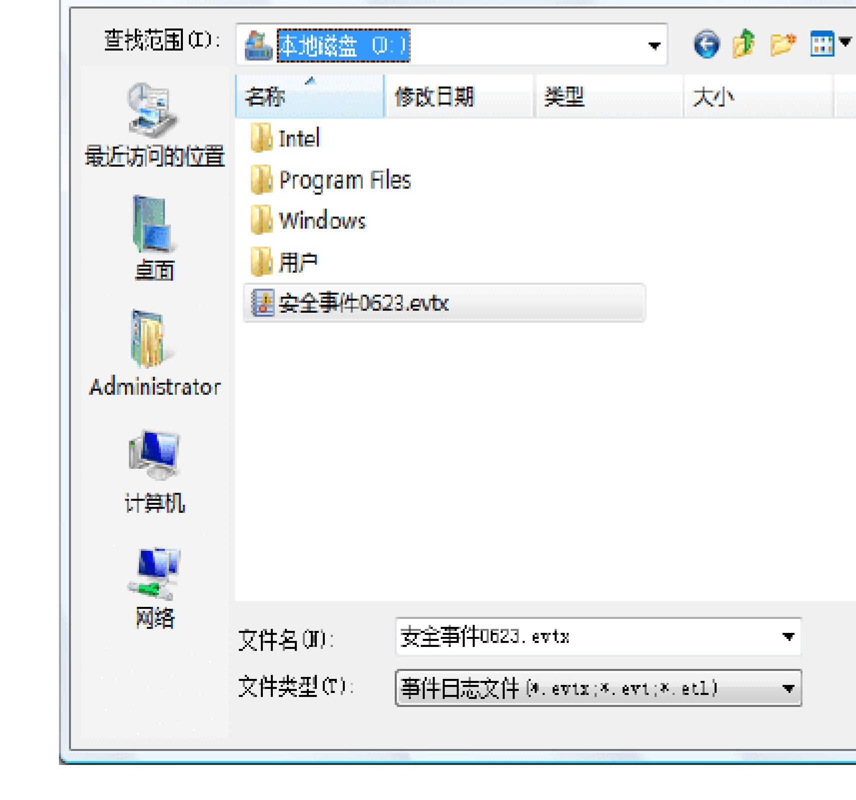
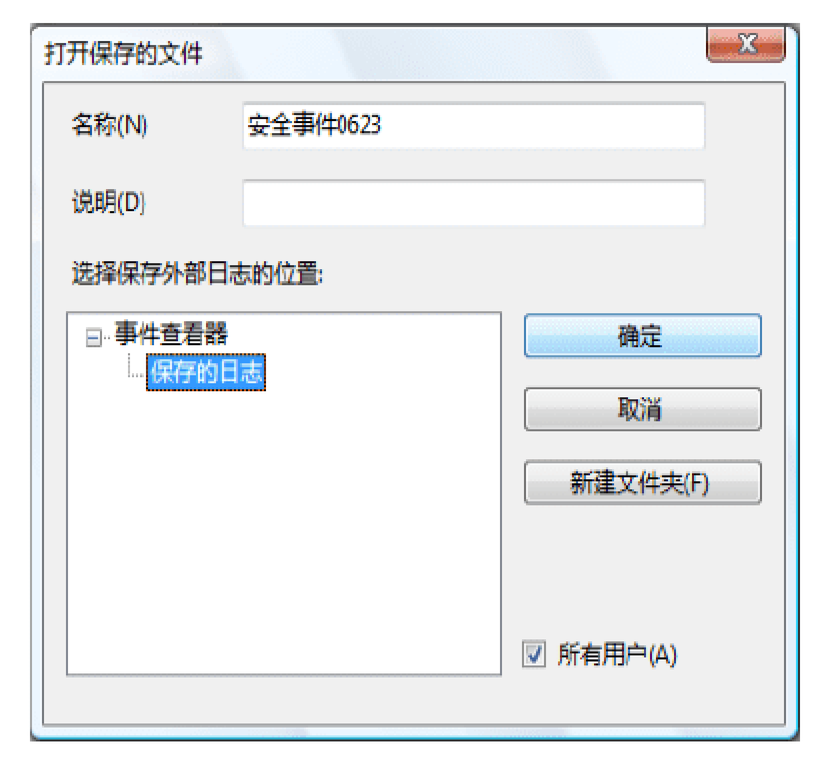


图13.21 “打开保存的文件”对话框

06 单击“打开”按钮，显示如图13.22所示“打开保存的文件”对话框，默认将在“事件查看器”导航栏中创建“保存的日志”项目，用于保存所有导入事件文件。选中“所有用户”复选框，本地计算机上的所有用户均可以通过事件查看器查看当前文件，取消则只有本地管理员帐户可以查看该文件。

07 单击“确定”按钮，即可添加到“事件查看器”窗口中，如图13.23所示。



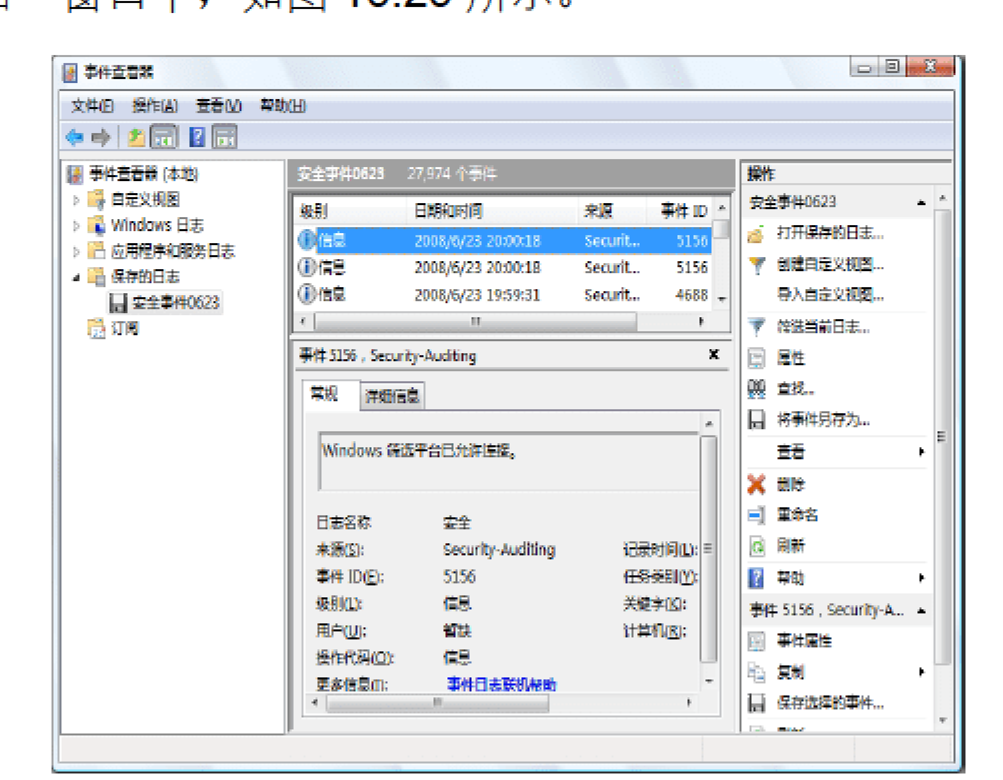


图13.22 “打开保存的文件”对话框　　图13.23 导入的事件日志





13.3　系统日志

在 Windows Server 2008 系统中，日志系统是一个非常重要的功能组成部分。系统日志可以记录下系统所产生的所有行为，并按照某种规范表达出来。使用日志系统所记录的信息为系统进行排错，优化系统的性能，或者根据这些信息调整系统的行为。在安全领域，日志系统的地位更加重要。

13.3.1　事件日志基本信息

通常情况下，计算机存储的日志类型包括 Windows 系统日志、服务器角色日志、应用程序和服务日志。其中，Windows 系统日志是系统默认的，包括应用程序、安全、安装程序、系统和转发的事件等 5 部分，服务器角色日志和应用程序日志取决于当前服务器运行服务和应用程序。

事件日志类似于日记，主要用于记录某一系统事件发生的日期、时间等基本信息，事件是操作系统在某一时刻对某一系统资源或者网路资源发生的访问操作，而记录的一系列行为，该行为包含当前的日期、时间、用户、计算机、来源、事件、类型、分类等信息。表 13.11 中显示了事件的基本要素及描述。

表 13.11　事件基本信息

要素	描述
日期和时间	事件发生的日期和时间。事件的日期和时间以协调通用时间（UTC）存储，但始终按查看者的区域设置显示
用户	事件发生所代表的用户的名称。如果事件实际上是由服务器进程所引起的，则该名称为客户 ID；如果没有发生模仿的情况，则为主 ID。在可用时，安全日志条目包括主 ID 和模仿 ID。当该服务器允许一个进程采用另一个进程的安全属性时，则产生模仿
计算机	产生事件的计算机的名称。这通常是您自己的计算机的名称，除非您在另一台计算机上查看事件日志
来源	记录事件的应用程序，它可为程序名（如"SQLServer,"）、系统的组件（如驱动程序）或大程序的组件。例如，"Elnkii"指示 EtherLinkII 驱动程序。“来源”始终使用其原始语言
事件 ID	标识此来源的特定事件类型的数字。说明的第一行一般包含事件类型的名称。例如，6005 是在启动事件日志服务时所发生事件的 ID。这类事件说明的第一行是“事件日志服务已启动”。通过结合使用“来源”和“事件”的值，产品支持代理可解决系统问题
级别	事件严重性的分类，包括信息、警告、错误、关键、Success Audit、审核失败等 6 个级别。在“事件查看器”中的正常列表方式下查看，它们都由一个符号表示
操作代码	包含标识活动或应用程序引起事件时正在执行的活动中的点的数字值。例如，初始化或关闭
日志	已记录事件的日志的名称
任务类别	用于表示事件发行者的子组件或活动
关键字	可用于筛选或搜索事件的一组类别或标记，包括“网络”、“安全”或“未找到资源”

13.3.2 系统日志概述

Windows 日志除包括早期版本的 Windows 中可用的日志（应用程序、安全和系统日志）之外，还包括两个新的日志类别，即安装程序日志和转发的事件日志。Windows 日志用于存储来自旧版应用程序的事件以及适用于整个系统的事件。应用程序日志包含由应用程序或程序记录的事件，主要记录程序运行方面的事件。

1. Windows 系统日志

Windows Server 2008 系统日志类包括如下 4 种：

- 应用程序日志。应用程序日志包含由应用程序或系统程序记录的事件。例如，数据库程序可在应用程序日志中记录文件错误。应用程序开发人员决定记录哪些事件；
- 安全日志。安全日志记录诸如有效和无效的登录尝试等事件，以及记录与资源使用相关的事件，如创建、打开或删除文件或其他对象。例如，如果已启用登录审核，登录系统的尝试将记录在安全日志中；
- 系统日志。系统日志包含 Windows 系统组件记录的事件。例如，在启动过程中加载驱动程序或其他系统组件失败将记录在系统日志中。服务器预先确定由系统组件记录的事件类型；
- 安装程序日志。安装程序日志，记录在系统安装或者安装微软公司的产品时，产生的系列事件，如果安装出现错误，可以使用此日志分析出现的问题。

运行 Windows Server 2008 操作系统且配置为域控制器的计算机，以另外 3 种日志记录事件：

- 目录服务日志。目录服务日志包含 Active Directory 服务记录的事件。例如，在目录服务日志中记录服务器和全局编录间的连接问题；
- 文件复制服务日志。文件复制服务日志包含 Windows 文件复制服务记录的事件。例如，在文件复制日志中，记录着文件复制失败和域控制器（利用关于系统卷更改的信息）更新时发生的事件。运行 Windows 并配置为域名系统（DNS）服务器的计算机在其他日志中记录事件；
- DNS 服务器日志。DNS 服务器日志包含 DNS 服务记录的日志。

另外，根据所安装服务的情况，计算机可能会提供其他类型的事件和事件日志。

2. 安全日志

安全日志包含诸如有效和无效的登录尝试等事件，以及与资源使用相关的事件，如创建、打开或删除文件或其他对象。管理员可以指定在安全日志中记录什么事件。管理员可以使用组策略来启动安全性日志，或者在注册表中设置审核策略，以便当安全性日志满后使系统停止响应。

安装程序日志包含与应用程序安装有关的事件。

系统日志包含 Windows 系统组件记录的事件。例如，在启动过程中加载驱动程序或其他系统组件失败将记录在系统日志中。系统组件所记录的事件类型由 Windows 预先确定。



转发事件日志用于存储从远程计算机收集的事件。若要从远程计算机收集事件，必须创建事件订阅。

3. 应用程序和服务日志

应用程序和服务日志是一种新类别的事件日志。这些日志存储来自单个应用程序或组件的事件，而非可能影响整个系统的事件。

此类别的日志包括 4 个子类型：管理日志、操作日志、分析日志和调试日志。管理日志中的事件尤其受使用事件查看器解决问题的 IT 专业人士的关注。管理日志中的事件应该提供有关如何对事件做出响应的指南。

- 管理事件：这些事件主要以最终用户、管理员和技术支持人员为目标。管理通道中的事件指示问题以及管理员可以操作的良好定义的解决方案。管理事件的示例之一是应用程序无法连接到打印机时所发生的事件。这些事件或者有详细文档记录，或者有与其关联的消息直接指导读者纠正问题所必须做的事情；
- 操作事件：操作事件用于分析和诊断问题或发生的事件。这些事件可以用于基于问题或发生的事件触发工具或任务。操作事件的示例之一是在从系统中添加或删除打印机时所发生的事件；
- 分析事件：分析事件是大量发布的事件。这些事件描述程序操作并指示用户干预所无法处理的问题；
- 调试事件：调试事件由开发人员用于解决其程序中的问题。

13.3.3　系统日志设置

系统日志有如此重要的作用，如何妥善保存这些日志记录，就成为管理员日常维护的一项重要工作。默认状态下，系统日志的存储空间、保存方法及保存日期都是有一定限制的，如果系统事件较多，时间长了很可能会造成存储溢出，即导致部分事件记录被自动清除。因此，通常情况下需要对系统日志进行如下设置。

1. 设置系统日志选项

在“事件查看器”控制台中，右击需要配置选项的日志类型，如“应用程序”事件日志，在快捷菜单中选择“属性”选项，显示如图 13.24 所示“系统 属性”对话框。包括如下选项：

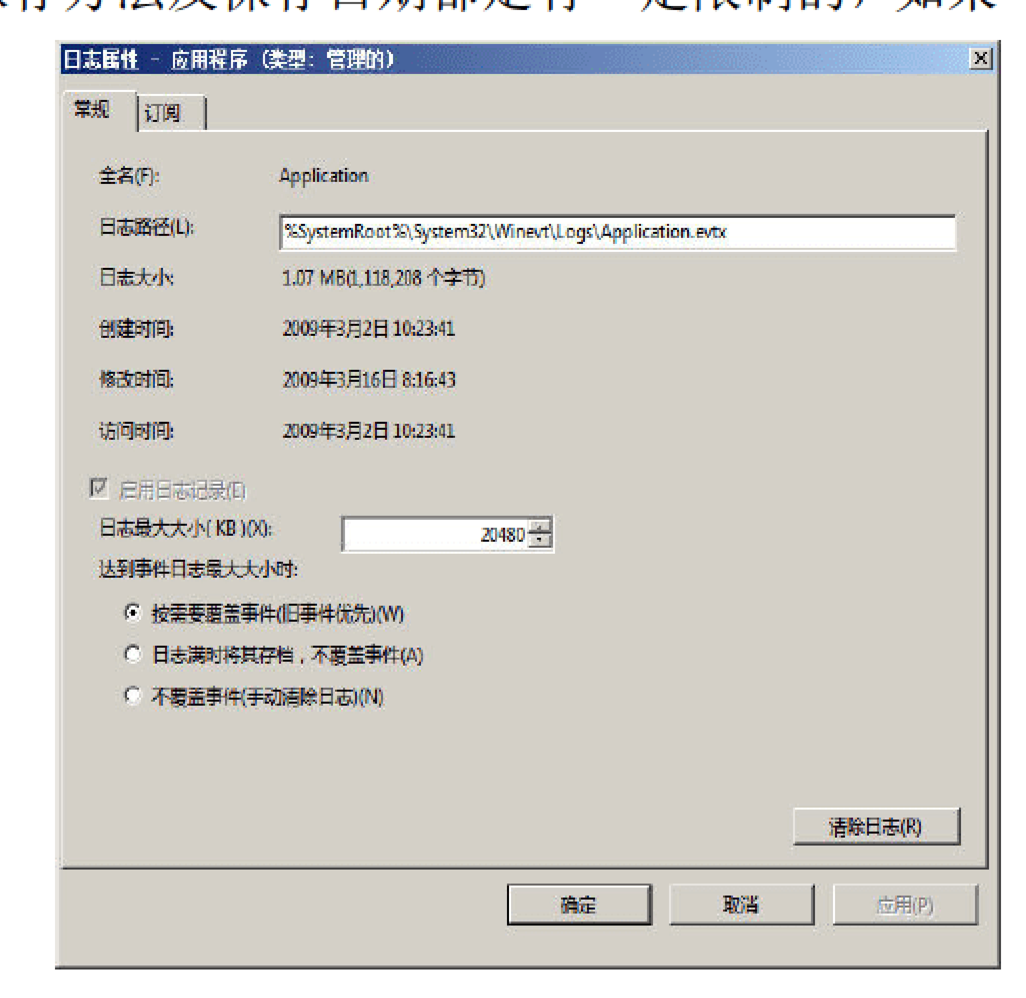


图 13.24　设置事件日志选项

- 日志路径：当前日志的保存路径；
- 日志最大大小：当前事件日志在计算机磁盘中被分配的磁盘空间，可以根据服务器类型判断日志文件的大小，从而设定合适

的空间上限，建议设置较大的空间上限，以免由于磁盘空间不足而自动删除未经保存的陈旧事件日志；

- 达到事件日志最大大小时：当达到日志大小上限时系统将按照默认或预先设定的动作执行，系统默认的是“按需要覆盖事件”。

2. 创建自定义视图

通常情况下，服务器运行过程中会产生大量的事件日志，逐个查看这些事件需要花费很长的时间，而其中大部分都是记录访问或操作成功的日志，对于管理员的安全管理工作意义不大。自定义视图的功能类似于“筛选”，通过创建自定义视图，可以指定用户希望查看的事件。例如只显示错误事件和警告事件，正常的事件将不需要显示。

01 以管理员帐户登录服务器，打开“事件查看器”窗口，选择“自定义视图”类别，并在“操作”栏中单击“创建自定义视图”链接，显示如图 13.25 所示“创建自定义视图”对话框。

02 在“记录时间”下拉列表中选择日志产生的时间，系统默认为“任何时间”，用户还可以选择“前 1 个小时”、“过去的 24 小时”、“最后的 7 天”等时间，或者选择“自定义范围”，打开如图 13.26 所示“自定义范围”对话框，设置希望查看日志产生的时间范围。例如按照时间产生的时间设置，首先分别在“从”和“到”下拉列表中选择“事件时间”，然后再分别定义开始和截止的日期和时间即可。

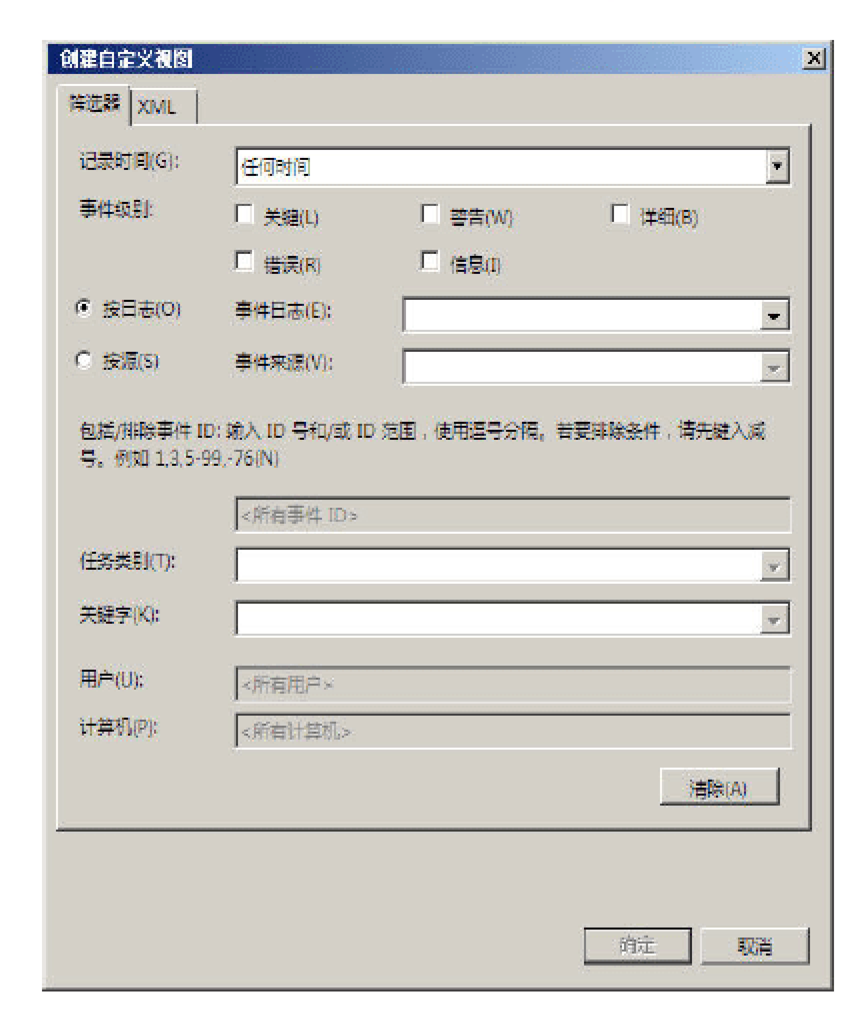



图 13.25 “创建自定义视图”对话框



图 13.26 “自定义范围”对话框

03 单击“确定”按钮返回“创建自定义视图”对话框，在“事件级别”选项区域选择事件的级别，例如“警告”和“错误”。选择“按日志”单选按钮，并在“事件日志”下拉列表中，依次选择“Windows 日志”→“安全”选项，如图 13.27 所示。

04 单击“确定”按钮，显示如图 13.28 所示“将筛选器保存到自定义视图”对话框，输入自定义视图的名称，以及自定义视图在事件查看器中的位置。



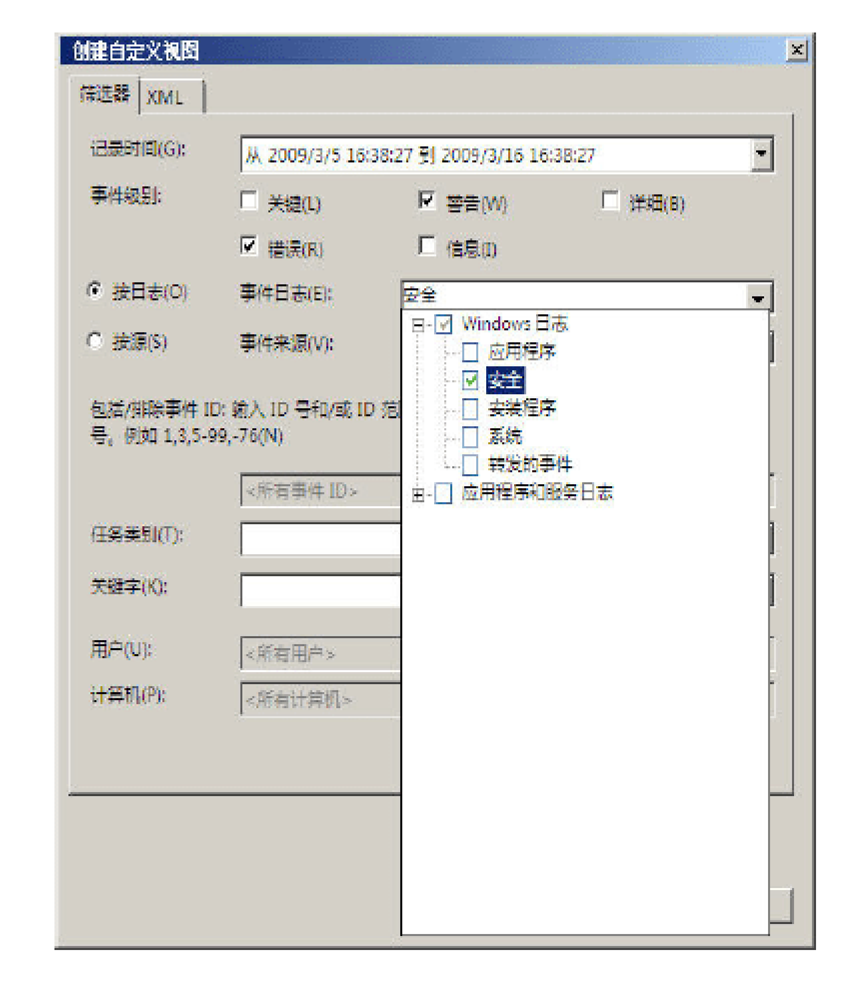


图 13.27　选择事件来源



图 13.28　“将筛选器保存到自定义视图”对话框

05 单击“确定”按钮，完成自定义视图的创建，如图 13.29 所示。在事件列表中，显示的事件级别全部是“错误”。

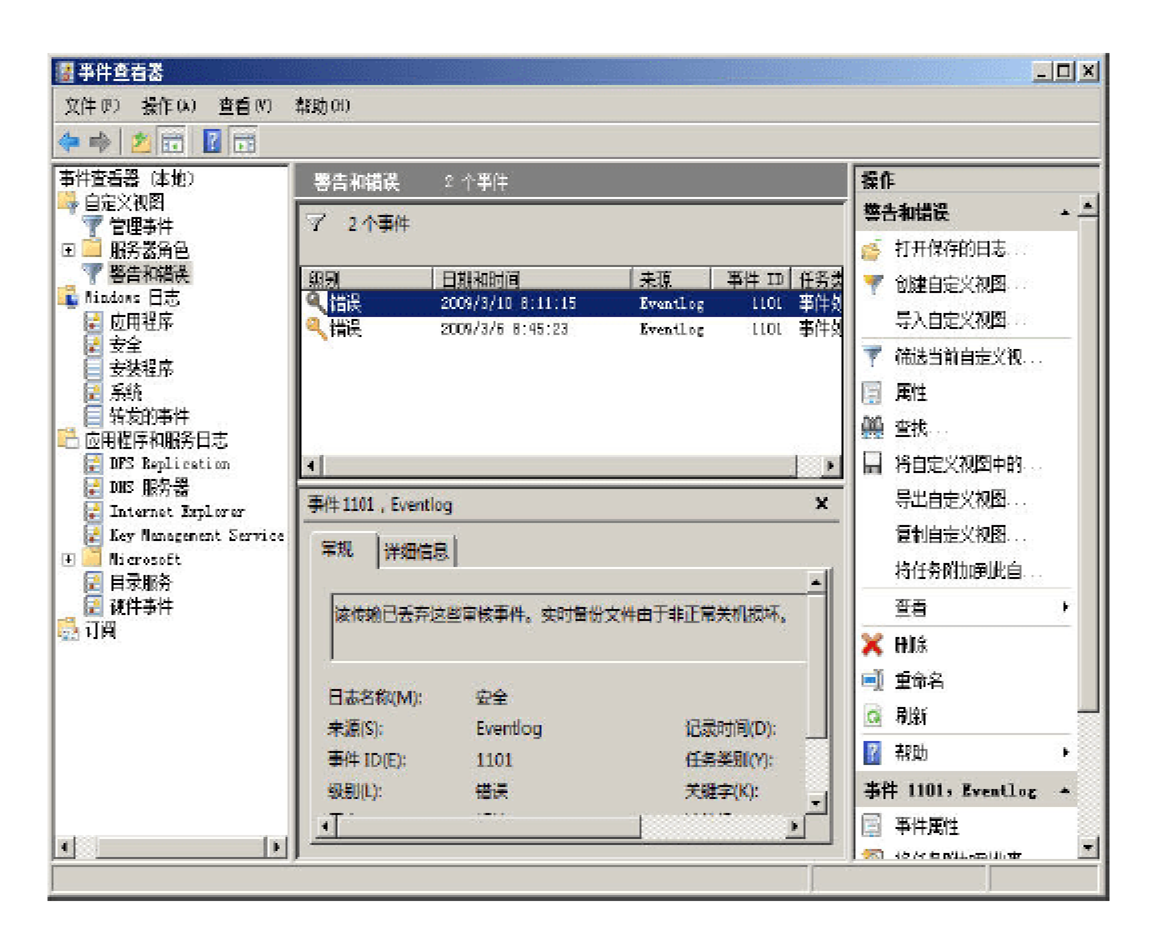


图 13.29　“警告和错误”窗口

3. 分析日志和调试日志

分析日志和调试日志主要面向 IT 专业用户，用于分析事件产生的原因、过程等因素，对普通用户的正常应用没有太大影响。因此，默认情况下分析日志和调试日志为禁用和隐藏状态。用户可以打开“事件查看器”窗口，然后选择“查看”菜单中的“显示分析和调试日志”命令，即可在“应用程序和服务日志”项目中看到相关的事件日志，如图 13.30 所示。

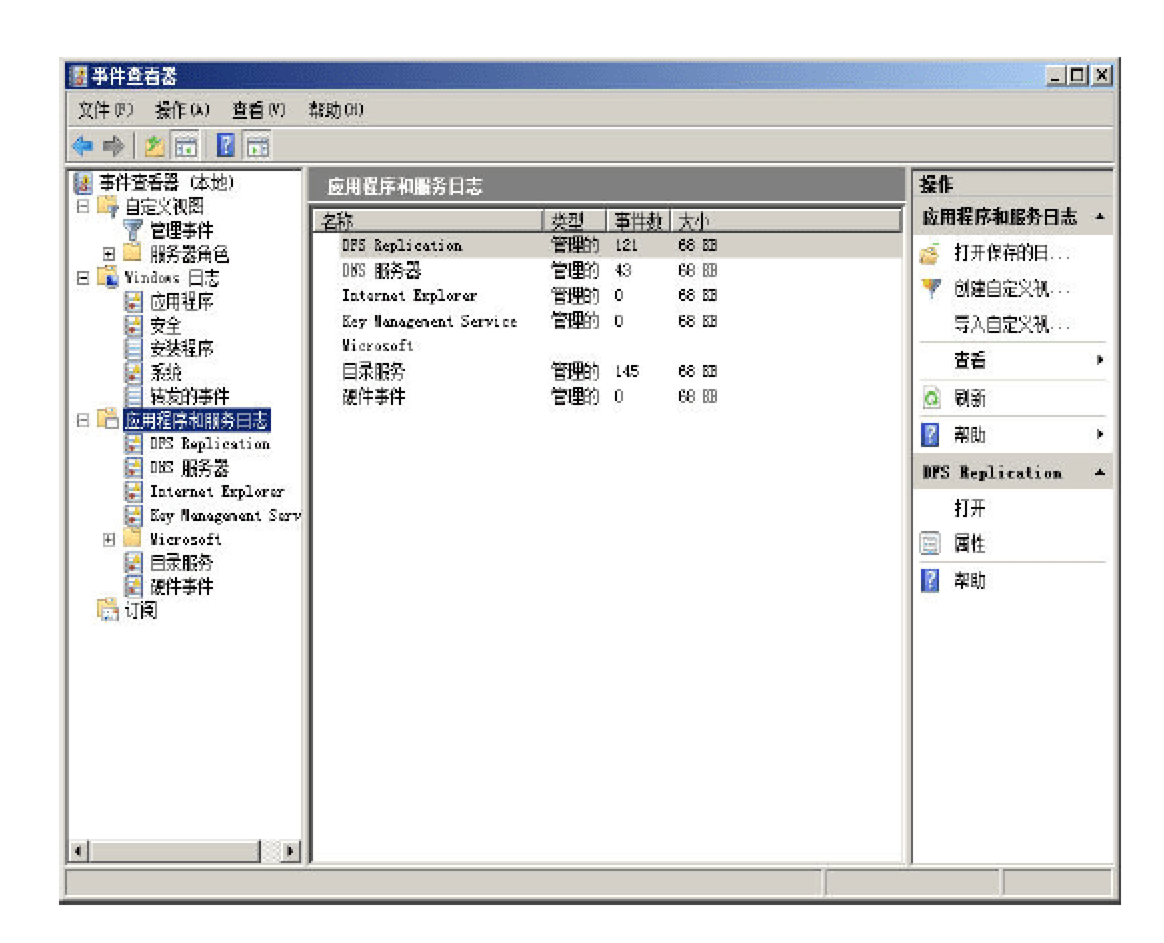


图 13.30　显示分析和调试日志

小　　结

系统事件审核策略是 Windows Server 2008 系统中的重要管理工具之一，也是每个系统管理员必须掌握的。系统审核策略虽然比较复杂，但是重要的是它可以帮助管理员从海量系统事件日志中，自动筛选出最具价值的信息。设置审核策略时，应注意仅启用最需要审核的策略类型，如果启用的审核策略过多甚至全部启用，将产生大量的审核事件日志。Windows 事件查看器可以帮助管理员查看和管理系统事件日志，而系统事件日志分别记录了各种系统应用和网络服务，在不同时刻的状态信息，是管理员了解系统运行状态、排查系统故障所必需的。

习　　题

1. 简述审核策略功能及应用。
2. Windows Server 2008 中的系统事件有哪些新特点？
3. 如何使用 Windows 事件查看器管理系统安全日志？

实验：使用自定义视图收集审核事件

实验目的

掌握 Windows Server 2008 事件查看器的应用。

实验内容

配置审核策略，并通过创建自定义视图，收集审核策略生成的事件。

实验步骤

1. 启用并配置审核策略。
2. 创建自定义视图。
3. 设置自定义范围。
4. 选择事件来源。
5. 将筛选器保存到自定义视图。
6. 查看自定义视图中收集的审核策略事件。

第14章

Internet 信息服务安全

IIS（Internet Information Service，Internet 信息服务）是一个统一的 Web 平台，其中包括 Web 服务器、FTP 服务器、NNTP 服务器和 SMTP 服务器，分别用于网页发布、文件传输、新闻服务和邮件发送等方面，为管理员和开发人员提供一个 Web 解决方案。如何加强 IIS 的安全机制，建立高安全性能的可靠的 WWW 服务器，已成为网络管理的重要组成部分。

本章导读

- IIS 7.0 安全特性
- Web 数据安全
- Web 访问安全
- Web 服务器常规安全设置
- 使用 SSL 证书配置安全 Web 站点
- FTP 服务安全

14.1　IIS 7.0 安全特性

IIS 7.0 是 Windows Server 2008 系统默认集成的 IIS 组件版本。相对于早期版本而言，IIS7.0 的安全性有明显提高，同时提供多种安全机制，包括基于 Windows 系统的基本身份验证方法以及基于域的高级身份验证方法。另外 IIS 7.0 采取完全模块化的安装和管理，增强了安全性和自定义服务器，减少攻击的可能，简化诊断和排除功能。

14.1.1　IIS 7.0 的新特性

IIS 7.0 是一个完全模块化的 Web 服务器，解决了老版本上的用户并不常使用特性过多对于代码的影响，性能方面有时不能让用户满意和由于默认的接口过多所造成的安全隐患。IIS 7.0 在 IIS 6.0 的基础上有了很大的功能改进，主要有：

- 更简便的命令行配置功能；
- 更强的兼容性；
- 抛弃 MetaBase；
- 集中管理；
- 委任配置；
- AppCmd 与其它新的管理手段；
- 失败请求追踪；
- 请求过滤；
- UNC 内容支持；
- 动态内容输出缓存。

14.1.2　IIS 7.0 访问控制安全

通过为服务器配置适当的身份验证机制，可以确认任何请求访问网站的用户的身份，以及授予访问站点公共区域的权限，同时还可以防止未经授权的用户访问专用文件和目录。除此之外，IIS 7.0 本身还提供了许多全新安全功能，如访问控制、IIS 管理器权限、授权规则等。

- .NET 信任级别。管理员可以通过此项安全设置为托管模块、管理程序和应用程序指定信任的级别，以提高网络组件和服务器的安全。该功能需要.NET 扩展组件的支持；
- IIS 管理器权限。该功能可以控制允许连接到网站或应用程序的用户对象，包括 IIS 管理器用户、Windows 用户或 Windows 组的成员。该功能仅适用于服务器连接。如果在 IIS 管理器中的服务器级别打开此功能，可以查看被授予了 Web 服务器上所有网站和应



用程序权限的用户，并且可以选择用户以删除该用户的网站或应用程序权限，提高服务器的安全性；
- IIS 管理器用户。通过该功能可以管理被允许连接到 Web 服务器上的网站或应用程序的用户帐户。IIS 管理器凭据默认已经内置于 IIS 中，无法被 Windows 或服务器上的任何其他应用程序识别；
- 访问控制。与 IIS 6.0 中的“IP 地址和域名限制”功能类似，可以通过配置“允许”或“拒绝”访问服务器的 IP 地址或域名列表，实现对服务器的访问控制；
- ISAPI 和 CGI 限制。该功能可以指定，允许在 IIS 服务器上运行的 ISAPI 和 CGI 组件。CGI 是最常用的 Web 服务器功能的扩展，主要用于搭建动态网站环境；
- 服务器证书。证书可以用来建立安全套接字层（SSL）连接，也可以用于验证来访用户帐户的身份；
- 功能权限委派。在 Windows Server 2008 中，管理员可以使用功能权限委派，为 WWW 服务器上的网站和应用程序，配置 IIS 管理器功能的委派状态。从 IIS 管理器中配置功能的委派状态时，可以指定该功能在 IIS 7.0 的服务器级别配置文件中，是否处于锁定状态。如果某项功能被锁定，则只能从（向）服务器级别配置文件中，读取（写入）该功能的配置。但是，如果希望从（向）较低级别的配置文件（如网站或应用程序中的 Web.config 文件）中，读取（写入）配置时，则可以解除锁定；
- 管理服务。管理员可以使用功能配置 IIS 管理器的管理服务。利用管理服务，计算机和域管理员可以通过远程方式，管理 Web 服务器、站点和应用程序；
- 身份验证。IIS 7.0 可以提供 7 种身份验证方法，并且集成 Active Directory 服务的身份验证机制，如 AD 客户端身份验证、摘要式身份验证等，以及.NET 组件提供的 ASP.NET 模拟身份验证方法等；
- 授权规则。管理员通过为服务器配置相应的授权规则，可以指定授权用户访问网站或应用程序的规则。

14.1.3　NTFS 访问安全

NTFS 文件系统可以为数据提供安全和访问控制，可以限制用户和服务对文件和文件夹的访问。使用 NTFS 文件系统时，必须为用户帐户授予相应的 NTFS 权限，该用户才能访问相应的文件或文件夹，否则就无法访问，从而在一定程序上保护了数据的安全。需要注意的是，NTFS 的安全性在本地计算机或网络中都是有效的。无论是以用户身份登录到服务器，还是通过网络访问共享文件夹，NTFS 安全性都有效。因此，从安全性角度考虑，应为 IIS 设置 NTFS 权限。

无论使用 IIS 搭建 Web 服务还是 FTP 服务，都应将文件存储在 NTFS 分区内，并利用 NTFS 权限来增强数据的安全性。在资源管理器中，右击 IIS 的安装目录（默认为%Systemroot%\Inetpub）选择快捷菜单中的“属性”选项，打开“inetpub 属性”对话框，切换到“安全”选项卡，单击“编辑”按钮，即可修改用户或组的访问权限，如图 14.1 所示。

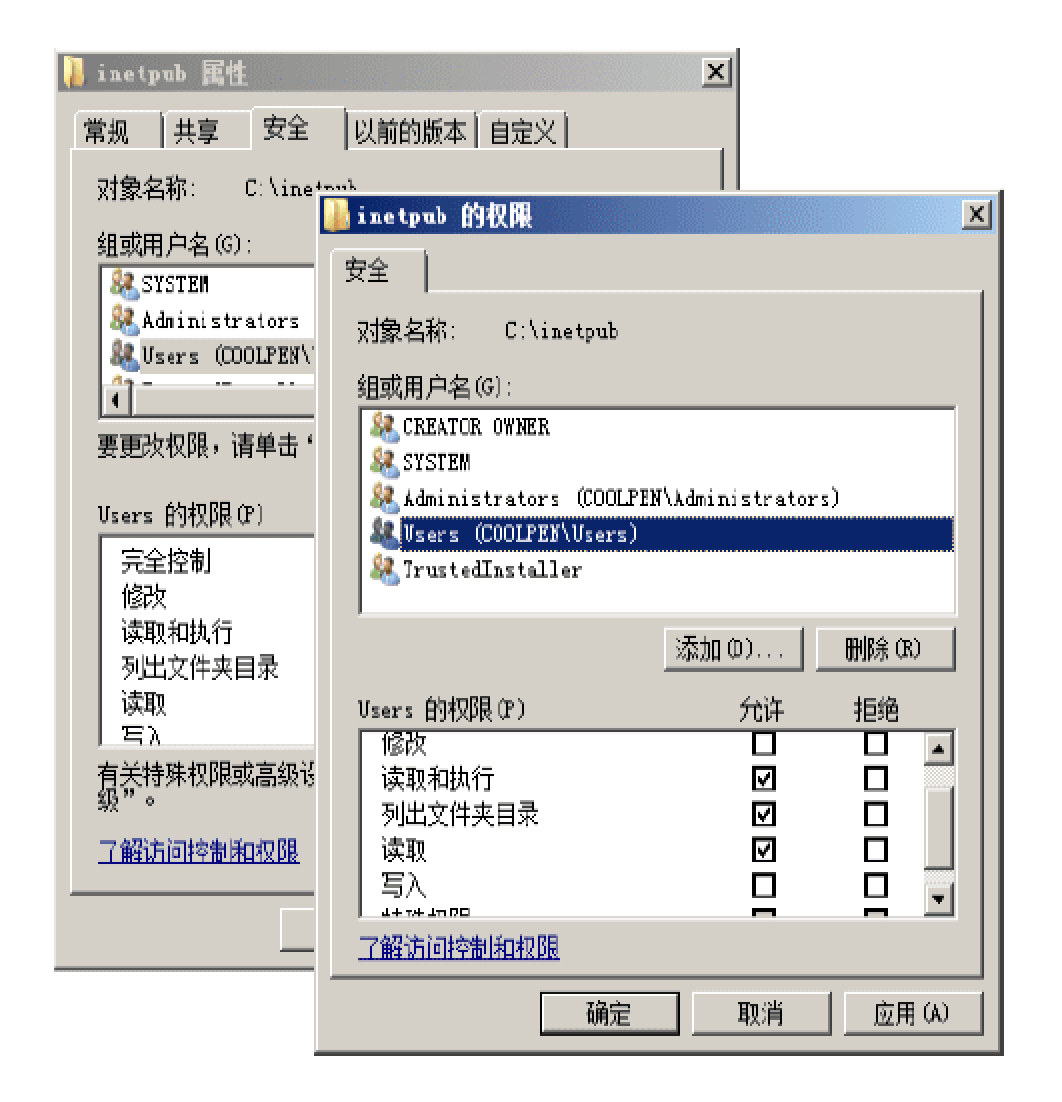


图 14.1　设置 NTFS 权限

如果 NTFS 的权限设置与 IIS 权限设置发生冲突，以最严格的设置为准。例如，NTFS 的权限设置为只读，而 IIS 权限设置为完全控制，那么用户的访问权限将只能是“只读”。为了使服务器尽可能地安全，应该重新检查一下所有 IIS 文件夹的安全设置并进行适当的调整。

14.1.4　IIS 7.0 安装安全

在安装 IIS 7.0 时应注意以下问题：

- 选择非域控制器作为 IIS 服务器。安装 IIS 过程中，系统将自动创建“IUSR_计算机名”匿名帐户，如果所选服务器是域控制器，则该用户帐户将被添加到域用户组中（Users），从而把应用于组的访问权限，就会提供给访问 IIS 服务器的每个匿名用户，这不仅给 IIS 带来潜在危险，而且还可能威胁整个网络的安全；
- 选择非系统分区作为安装目录。把 IIS 安装在系统分区上，会使系统文件与 IIS 同样面临非法访问，容易使非法用户侵入系统分区，所以在安装 IIS 的 Web、FTP 等服务时，应尽量避免将 IIS 服务器安装在系统分区上；
- 安装在 NTFS 类型分区上。相对于 FAT32 分区而言，NTFS 分区拥有较高的安全性和可管理性，并且磁盘利用效率高，可以设置复杂的访问权限，以适应不同信息服务的需求；
- 只安装必需的组件。除非特别需要，否则不要安装 Internet 打印以及 ASP.NET、CGI 等动态网站扩展组件，以避免恶意用户借助相应的组件漏洞或设置错误，实现对 IIS 服务器的攻击；
- 定制自己需要的安全功能组件。IIS 7.0 提供的更为丰富的安全功能设置，管理员可以根据 IIS 服务器的需求定制适当的安全限制。



14.2　Web 数据安全

Web 网站被黑、FTP 资源被恶意删除等安全事件屡见不鲜，如何确保网站安全运行，已经成为网络管理员的重要任务之一。IIS 7.0 提供了众多的身份验证机制，可以在恶意用户入侵途中发挥相应的作用，但是一旦主动防御措施失效，后果将不堪设想。为此管理员还必须确保 Web 站点内容的安全，即做好备份工作和日志管理工作。

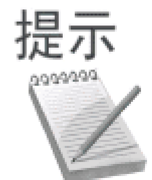
14.2.1　IIS 7.0 配置备份和还原

随着 Web 网站功能和页面的不断增加，各种目录和虚拟目录就会比较多，配置会越来越复杂。如果发生网络入侵或服务器故障，可能造成无法挽回的损失。在 IIS 7.0 以前版本中 IIS 都自带了备份和恢复设置功能，而 IIS 7.0 的系统配置文件，完全采用一个 XML 配置文件来完成，管理员可以拷贝来备份、还原和修改 IIS 的设定。IIS 7.0 将全局配置文件存储在%SYSTEMROOT%\system32\inetsrv\config\Application Host.config 文件中。此 XML 文件包含两个主要的配置节组：

- system.applicationHost 节组包含站点、应用程序、虚拟目录以及计算机上的应用程序池的设置，无论它们是否是 Web 服务器的一部分；
- system.webServer 节组包含计算机上 IIS 7.0 Web 服务器的全部配置设置。例如，该节组是在 Web 服务器上配置全局 Web 服务器默认值、Web 服务器安全性以及 HTTP 文件压缩的位置。也可以在此文件中存储特定站点或应用程序的配置设置。

由于 IIS 7.0 配置是基于 Microsoft .NET Framework 配置的，因此可以使用 web.config 文件同时存储 IIS 7.0 和 ASP.NET 配置设置。此 XML 文件包含 Web 服务器上的网站、Web 应用程序、URL、物理或虚拟目录的本地配置设置。此文件存储在网站或 Web 应用程序的代码和内容所存储的目录里。

提示



由于 IIS 7.0 配置文件被写入为 XML 文件，因此可以使用文本编辑器或 Microsoft Visual Studio 对其进行编辑。

14.2.2　IIS 7.0 日志记录

除了 Windows 提供的日志记录功能以外，IIS 7.0 还可以提供其他日志记录功能。例如设置日志文件格式并指定要记录的请求。IIS 日志数据可以记录服务器和每个网站的访问，通过该日志可以了解服务器和网站的运行情况，发现和排除潜在威胁。

如果用户希望 IIS 能基于配置的条件有选择地记录特定的服务器请求，应该开启服务器日

志记录。一旦启用了服务器的日志记录，就可以为服务器上的任意站点启用选择性日志记录。管理员可以查看日志文件，以了解失败和成功的请求。下面以设置 Default Web Site 站点日志为例讲解 IIS7.0 日志设置方法。

01 在“Internet 信息服务（IIS）管理器”窗口中，打开“Default Web Site 主页”，双击“日志”图标，显示如图 14.2 所示“日志”窗口。在日志文件格式列表框中选择“W3C”格式，其中日志文件的格式有 4 种，分别是：

- IIS。将 IIS 配置为使用 Microsoft IIS 日志文件格式来记录有关网站的信息。这种格式由 HTTP.sys 进行处理，并且是固定的基于 ASCII 文本的格式，这意味着用户无法自定义记录的字段。时间记录为本地时间，字段由逗号分隔；
- NCSA。将 IIS 配置为超级计算机应用程序国家中心公用日志文件格式来记录有关网站的信息。这种格式由 HTTP.sys 进行处理，是一种固定的 ASCII 格式，字段由空格分隔，时间记录为本地时间；


图 14.2 “日志”窗口

- W3C。使用 W3C 扩展日志文件是可自定义的基于 ASCII 文本的格式，用户可以指定记录的字段，字段由空格分隔，记录时间采用 UTC 格式；
- 自定义。将 IIS 配置为对自定义的日志记录模块使用自定义格式，如果选择此项，则“日志”页将被禁用，因为无法在 IIS 管理器中配置自定义日志。

02 单击“选择字段”按钮，显示如图 14.3 所示“W3C 日志记录字段”对话框。管理员可以根据实际情况进行相关设置。在“目录”文本框中设置日志保存的目录，默认保存的目录为：%SystemDrive%\inetpub\logs\LogFiles。在“日志文件滚动更新”选项框中，选择创建日志文件的方法。包括：

- 计划。设置更新的时间，例如每周更新；
- 最大文件大小。当日志文件达到该值是，自动更新日志文件；
- 不创建新的日志文件。将该目录下的所有网站日志都记录到单个文件中。

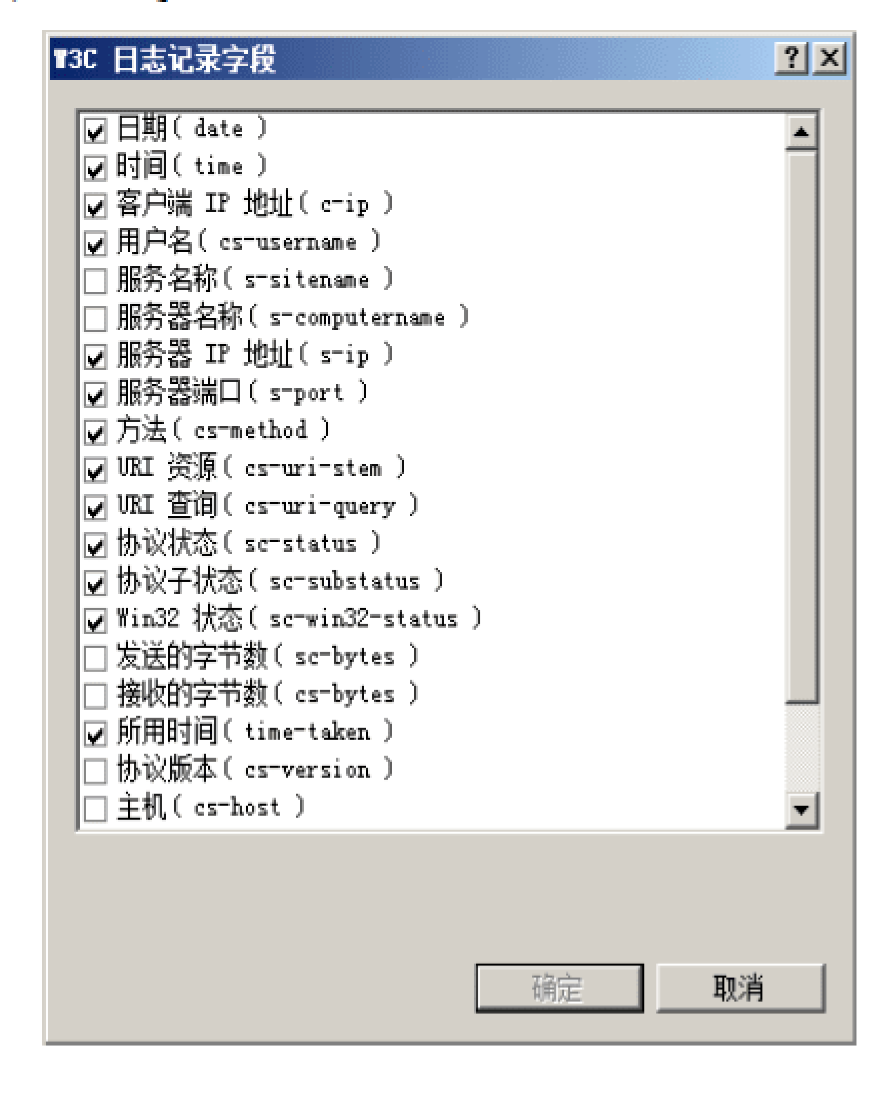


图 14.3 “W3C 日志记录字段”对话框

03 设置完后在“操作”栏中的单击“应用”选项完成日志设置。



14.3　Web 访问安全

IIS 7.0 新增了多种安全访问控制功能，可以满足用户各种网络环境的需求。另外，管理员可以对 Web 站点的主目录设置 NTFS 访问权限，从而对使用不同用户帐户的来访用户赋予不同的访问和操作权限，对于匿名用户则只赋予其最小有效权限即可，充分确保站点和服务器的安全。

14.3.1　设置 NTFS 访问权限

NTFS 文件系统是 Windows Server 2008 系统分区必需的，鉴于许多安全访问机制都是基于 NTFS 文件系统的，所以推荐所有分区均使用该文件系统格式化。对于 Web 站点而言，管理员只需对希望设置访问权限的站点主目录或虚拟目录设置 NTFS 访问权限即可。需要注意的是，设置过程中应注意 NTFS 访问权限自动继承和传播的特点，避免影响到其他站点或页面的正常访问。

01 以“company”文件夹为例。在 Windows 资源管理器中，右击“company”文件夹并选择快捷菜单中的“属性”选项，显示“company 属性”对话框。切换至“安全”选项卡，选择相应的组或用户，就可以看到该组或用户拥有的权限，如图 14.4 所示。

02 单击“编辑”按钮，显示如图 14.5 所示“company 的权限”对话框，管理员可以添加用户并设置相关权限，也可以更改权限。

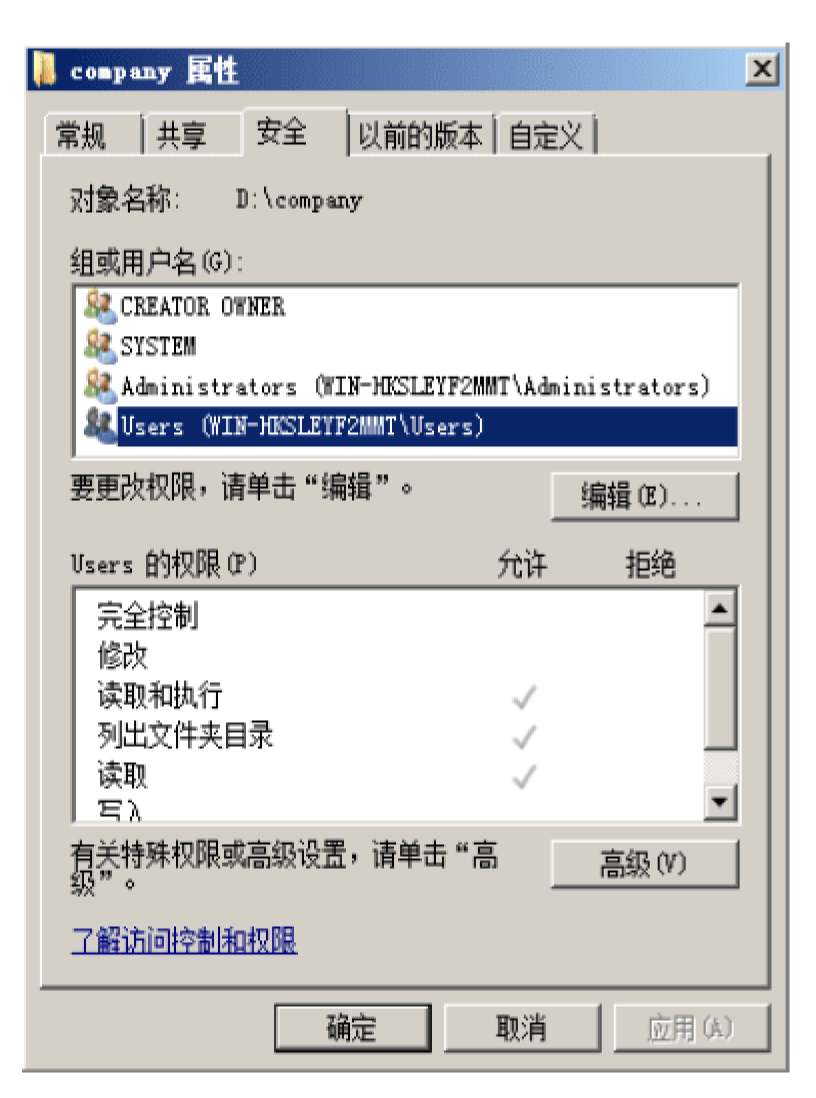


图 14.4　“company 属性”对话框



图 14.5　“company 的权限”对话框

03 设置完成后，单击“确定”按钮返回“company 属性”对话框。单击“高级”按钮，打开如图 14.6 所示“company 的高级安全设置”窗口，在这里可以更详细地设置文件夹权限。



图 14.6 “company 的高级安全设置”窗口



提示 兼有 IIS 权限和 NTFS 权限时，有效权限为两者的最小权限，如 IIS 权限设置为“完全控制”，而 NTFS 的权限设置为“只读”，那么用户最终的访问权限为“只读”。对于 NTFS 权限，文件权限优于文件夹权限。

14.3.2 设置身份验证方式

默认情况下 IIS 7.0 支持匿名身份验证和集成 Windows 身份验证。匿名身份验证允许任何用户访问公共内容，而不用向客户端浏览器提供用户名和密码质询。如果某些内容只给指定的用户查看，而且使用的是匿名身份验证，则必须设置相应的 NTFS 文件系统权限来防止匿名用户访问这些内容。如果希望只运行注册用户查看选定的内容，可以设置要求提供用户名和密码的身份验证方法，如摘要式身份验证或基本身份验证。

1. 配置匿名身份验证

启用匿名身份验证后，管理员可以更改 IIS 用户访问站点和应用程序的帐户。默认情况下，IIS 7.0 使用 IUSR 作为匿名访问的用户名。以 company 站点编辑匿名身份验证凭据为例。



图 14.7 “company 主页”窗口

01 在“Internet 信息服务管理”窗口中，依次选择“起始页”→“WIN-HKSLEYF2MMT（计算机名）”→“网站”→“Default Web Site”→“company”选项，显示如图 14.7 所示“company 主页”窗口。

02 在“company 主页”窗口中双击“身份验证”选项，打开“身份验证”窗口，右击“匿名身份验证”，在打开的快捷菜单中选择“编辑”命令，显示“编辑匿名身份验证凭据”对话框，单击“设



置”按钮，显示“设置凭据”对话框，输入希望使用的用户名和密码即可，如图 14.8 所示。

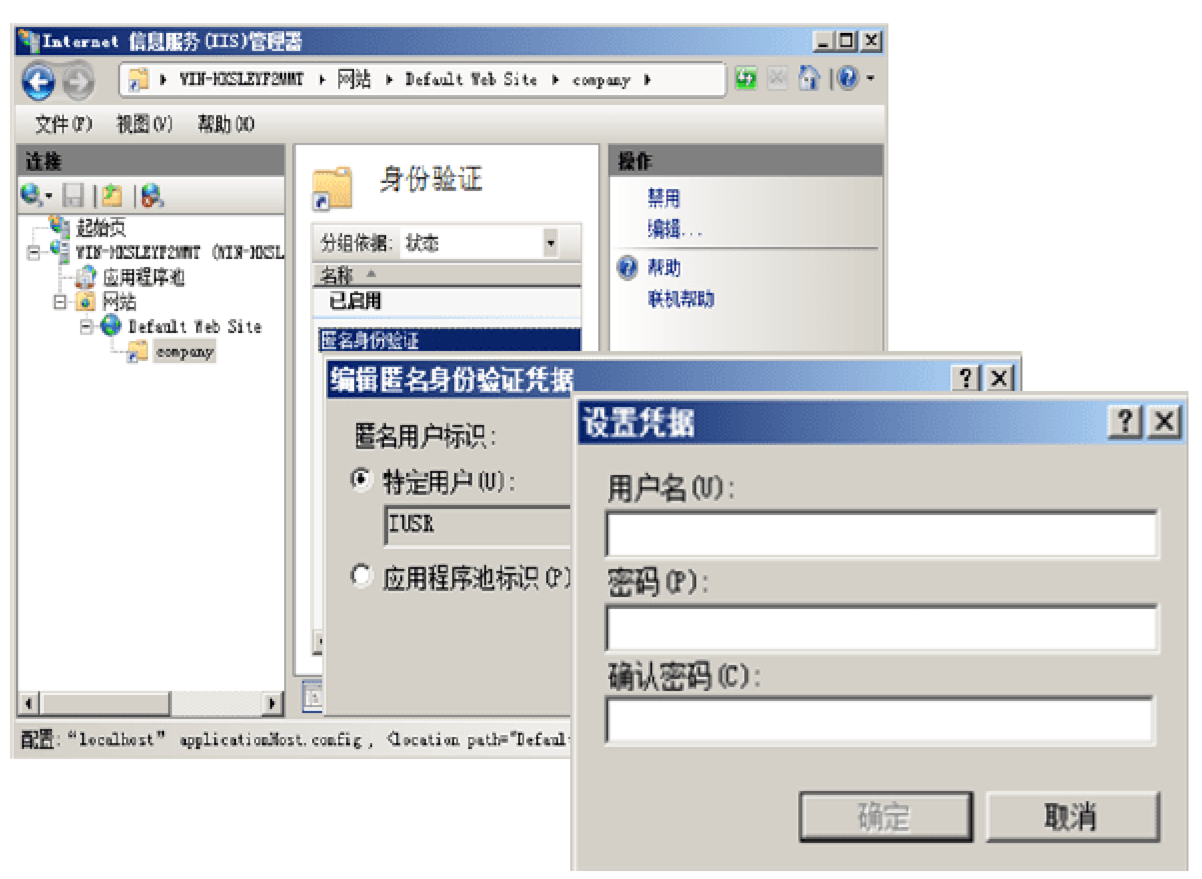


图 14.8　设置身份验证信息

03 依次单击“确定”按钮，保存设置即可。

2. 配置基本身份验证

基本身份验证要求用户提供有效的用户名和密码才能访问网站。这种身份验证方法可以跨越服务号和代理服务器，主流浏览器都支持这种身份验证方法。所以，当仅允许用户访问服务器上的部分内容而非全部内容时，可以使用这种方法。这里以为 company 网站配置 Windows 身份验证为例讲解设置方法。

01 打开 IIS 管理器，在 company 主页中双击“身份验证”，打开如图 14.9 所示“身份验证”窗口。右击“基本身份验证”选项，在弹出的快捷菜单中选择“启用”命令，启用基本身份验证。

02 右击“基本身份验证”选项，弹出选择快捷菜单中的“编辑”命令，显示如图 14.10 所示“编辑基本身份验证设置”对话框。在“默认域”文本框中输入一个默认域或将其留空。将根据对登录到该站点时未提供域的用户进行身份验证。在“领域”文本框中，输入一个领域或将其留空。一般而言，领域使用的是默认域的值。



图 14.9　“身份验证”窗口

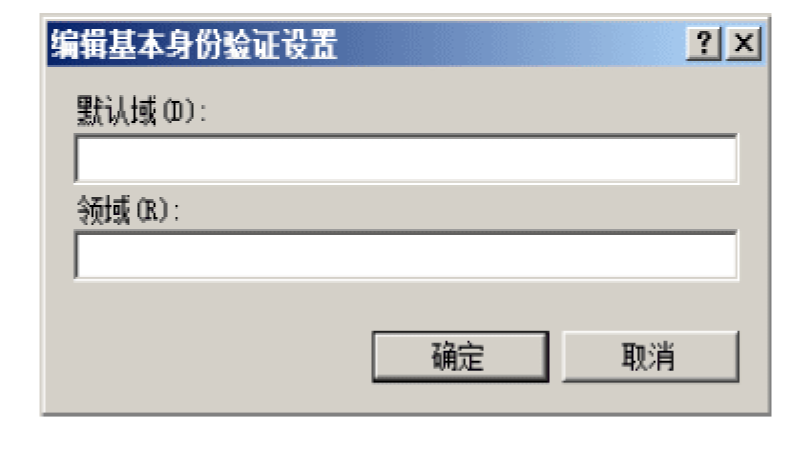
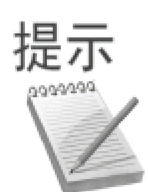


图 14.10　“编辑基本身份验证设置”对话框

03 依次单击“确定”按钮，保存配置即可。

提示  如果“领域”使用的是默认域，则在用户和密码质询期间，内部的域名可能会暴露给外部用户。

3. 配置摘要式身份验证

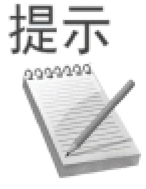
摘要式身份验证，是使用 Windows 域控制器对请求访问 Web 服务器内容的用户进行身份验证。当需要获得比基本省份验证更高的安全时，可以使用摘要式身份验证。

01 打开 IIS 管理器，在 company 主页中双击“身份验证”，打开“身份验证”窗口。右击“摘要式身份验证”选项，弹出选择快捷中的“启用”命令，启用“摘要式身份验证”。再右击“摘要式身份验证”选项，在弹出的快捷菜单中选择“编辑”命令，显示如图 14.11 所示“编辑摘要式身份验证设置”对话框。在“领域”文本框中输入 IIS 在对尝试访问受摘要式身份验证保护的资源的客户端进行身份验证时使用的领域。



图 14.11 “编辑摘要式身份验证设置”对话框

02 单击“确定”按钮，完成配置退出。

提示  摘要式身份验证要求将 Web 服务器加入某个域或该计算机是域服务器。如果要使用摘要式身份验证，必须禁用匿名身份验证。如果不禁用匿名身份验证，用户将可以通过匿名方式访问服务器上的所有的内容，包括受限制的内容。不支持 HTTP1.1 协议的任何浏览器都无法支持摘要式身份验证。

14.3.3 授权规则设置

通过配置 Web 站点的授权规则，可以指定允许授权用户访问网站和应用程序的规则，例如允许或拒绝指定用户或组访问网站等。这种授权规则，可以是基于用户帐户或组的，也可以是基于应用程序角色的。下面以为 zhangsan 添加拒绝访问规则为例讲解授权规则设置方法。

01 选择“开始”→“管理工具”→“Internet 信息服务管理器”命令，单击“company”选项，打开 company 主页。双击“授权规则”，打开如图 14.12 所示“授权规则”窗口，默认允许所有用户访问。

02 在“操作”栏中选择“添加拒绝规则”选项，显示如图 14.13 所示“添加拒绝授权规则”对话框。选中“指定的用户”复选框，输入“zhangsan”。





图 14.12　“授权规则”窗口

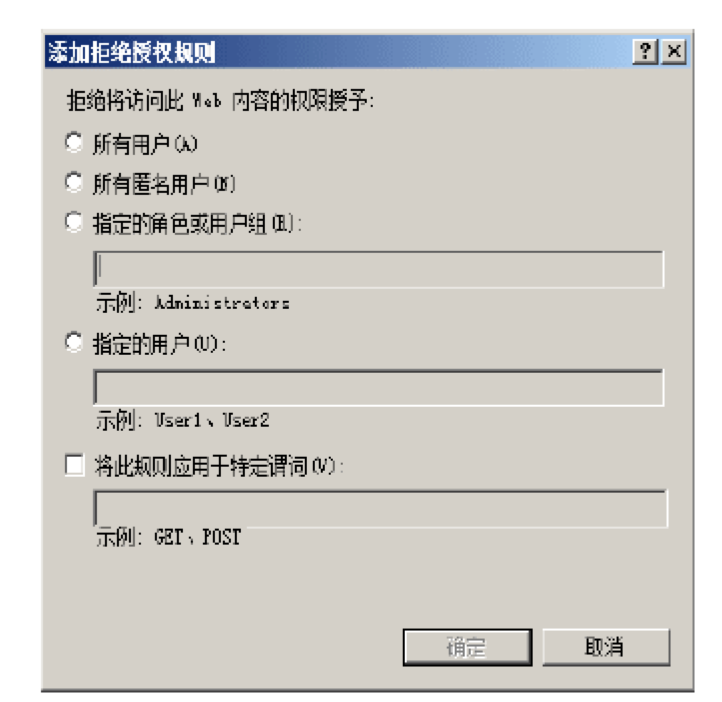


图 14.13　“添加拒绝授权规则”对话框

03 单击“确定”按钮，即可将新建规则添加到“授权规则”列表中。

14.4　Web 服务器常规安全设置

WWW 服务已经成为众多网络的必备服务，是提供信息发布、邮件查询、电子商务、网络办公等的网络平台。WWW 服务的安全直接决定多种网络服务的安全，甚至整个网络的安全。基于 IIS 7.0 的 WWW 服务本身已经集成了多种安全功能，用户只需通过简单配置，便可获得安全可靠的网络平台。

14.4.1　自定义错误

自定义错误是一把双刃剑，它是一个优秀的错误调试工具，可以提供站点出现问题的信息。某些自定义错误页可能会发布一些敏感的信息，容易引发危险。这里以为 company 添加一个错误页面并以 302 重定向相应到 http//www.contoso.com/404.aspx 为例。

01 在“Internet 信息服务管理器”窗口中，依次选择“WIN-HKSLEYF2MMT”→“网站”→“company”命令，显示如图 14.14 所示“company 主页”窗口。



图 14.14 “company 主页”窗口

02 双击“错误页”图标，在“错误页”窗口的“操作”栏中单击“添加”连接，显示如图 14.15 所示“添加自定义错误页”对话框。在“状态代码”文本框中输入状态代码，选中“以 302 重定向响应”单选按钮，输入“http：//www.contoso.com/404.aspx”。其中响应操作有 3 个选项，分别是：

- 将静态文件中的内容插入错误响应中。如果错误页包括静态内容（如 html），可以选择此项；
- 在此网站上执行 URL。如果错误页包括动态内容（如 asp），可以选择此项，在对应的“URL（相对于网站根目录）”文本框中输入自定义错误页的相对路径；
- 以 302 重定向响应。如果希望客户端被重定向到其他 URL，可以选择此项，在“绝对 URL”文本框中，输入重定向目标的完整 URL。

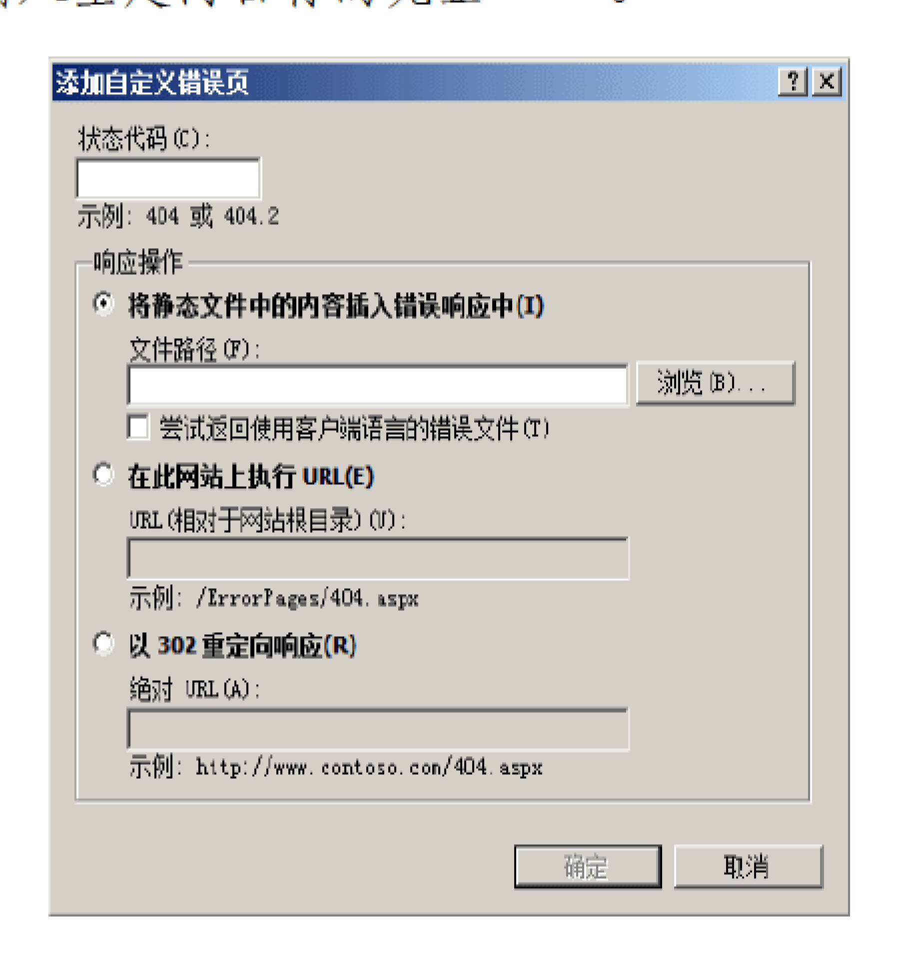


图 14.15 “添加自定义错误页”对话框

03 单击“确定”按钮，保存设置即可。



14.4.2 设置内容过期

“设置内容过期”是 Web 服务器重要的安全防护措施之一。对于时效性较强的数据信息（如会议通知、产品报价等），可以通过设置内容过期来更新所发布的内容。浏览器会自动比较当前日期与截止日期，如果发现内容已过期则不再发布该数据，客户端也不会显示缓存页面而是从服务器更新。

01 在“Internet 信息服务管理器”窗口中，打开系统默认站点（Default Web Site）主页，双击“HTTP 响应标头”图标，显示“HTTP 响应标头”窗口。在“操作”栏中，单击“设置常用标头”链接，显示 “设置常用 HTTP 响应头”对话框，选中“使 Web 内容过期”复选框，并设置相应的过期方式。如图 14.16 所示。

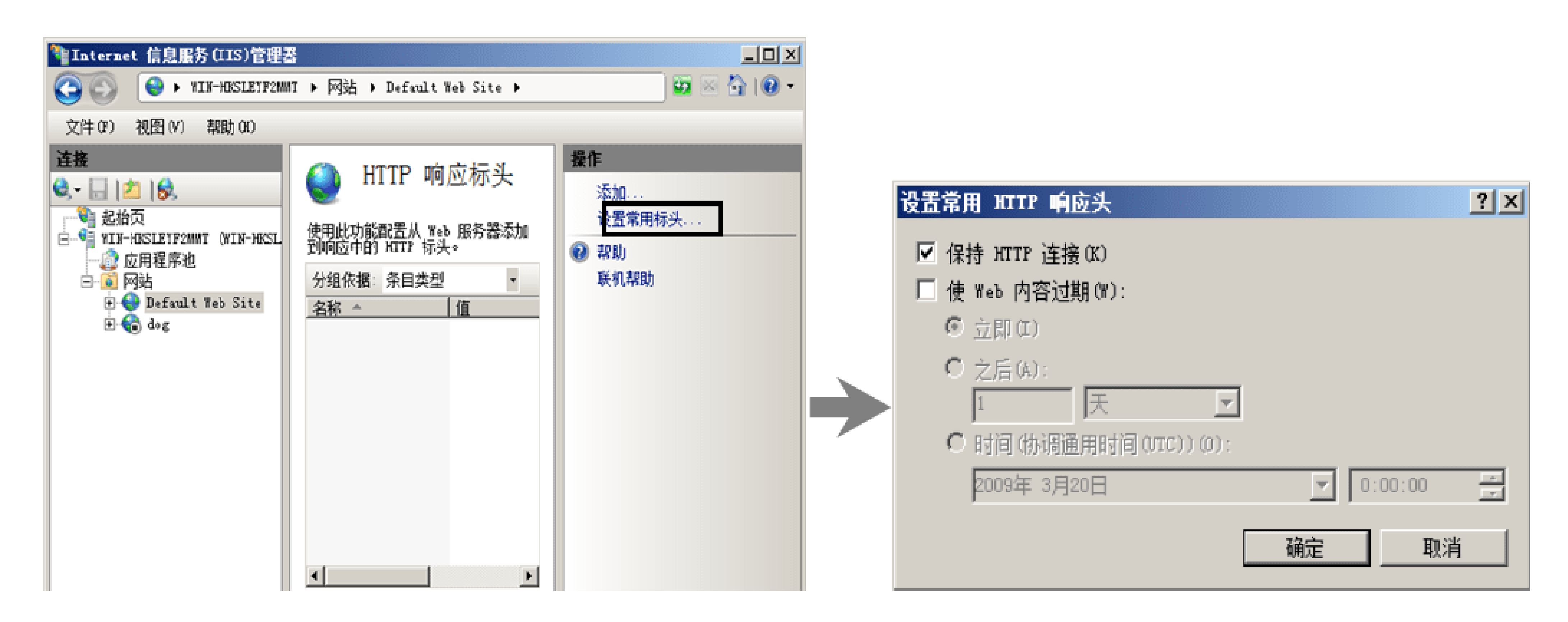


图 14.16 设置常用 HTTP 响应头

02 单击“确定”按钮，保存设置即可。

14.4.3 禁止目录浏览

如果开启目录浏览，访问者将可以看到网站的目录结构，可以防止黑客有针对性的破坏。下面以禁止 Default Web Site 站点的目录浏览为例介绍操作方法。

在“Internet 信息服务（IIS）管理器”窗口中，打开默认站点（Default Web Site）主页。双击“目录浏览”选项，显示如图 14.17 所示“目录浏览”窗口，如果启用目录浏览，访客可以看到文件的日期、大小、扩展名等信息，选中所有复选框，单击“禁用”链接，禁用目录浏览。



图 14.17 “目录浏览”窗口

提示　IIS 7.0 默认禁用目录浏览。

14.4.4　IPv4 地址控制

默认情况下，IIS 会自动检查每个来访者的 IP 地址，通过 IP 地址的访问来防止或允许某些特定的计算机、域，甚至整个网络访问站点。因此，通过 IP 地址限制来在 Internet 上排除未知用户是非常有效的方法。同时，IIS 7.0 还提供了基于 Windows 域的访问限制，管理员可以禁止或允许来自指定域的用户访问站点或目录，该功能默认是未启用的。

01 在“Internet 信息服务（IIS）管理器”的“Default Web Site 主页”窗口中，双击“IPv4 地址和域限制”图标，显示如图 14.18 所示“IPv4 地址和域限制”窗口。

02 单击“添加允许条目”链接，打开“添加允许限制规则”对话框。系统默认选择“特定 IPv4 地址”单选按钮，在对应文本框中，输入想要允许访问的单个 IP 地址即可。建议选择“IPv4 地址范围”单选按钮，并输入相应的主机 IP 地址和“掩码”，如图 14.19 所示，可以同时添加多个被允许访问的主机 IP 地址。




图 14.18　“IPv4 地址和域限制”窗口

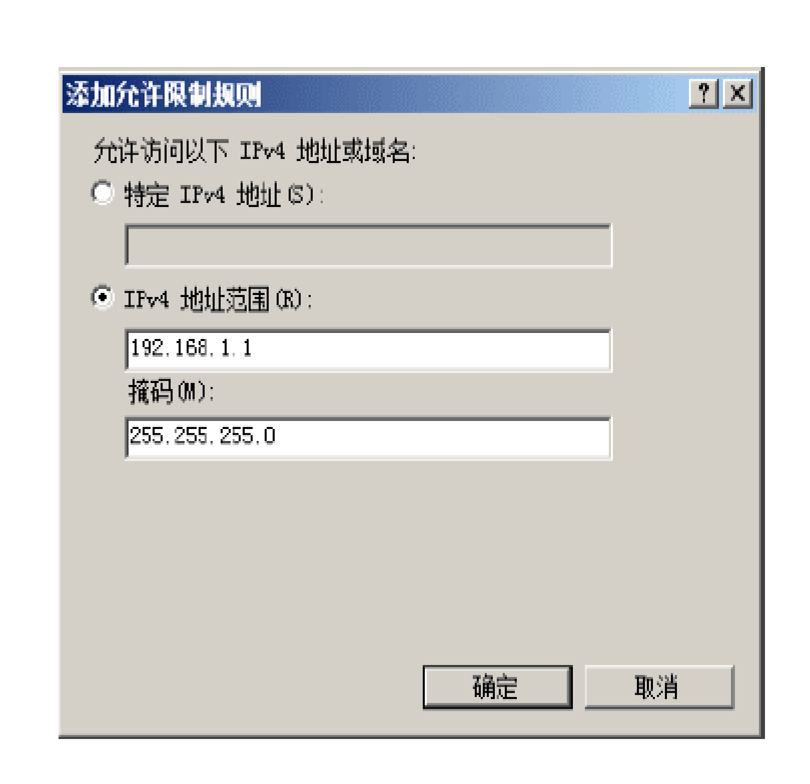


图 14.19　“添加允许限制规则”对话框

03 单击“确定”按钮，新创建的限制规则即可被添加到“IPv4 地址和域限制”列表中。“添加拒绝条目”的操作步骤与之类似，此处不复赘述。

04 在“操作”栏中单击“编辑功能设置”链接，显示如图 14.20 所示“编辑 IP 和域限制设置”对话框，用户还可以根据域名来限制要访问的计算机。在“未指定的客户端的访问权”下拉列表中，设置除指定的 IP 地址外的客户端，访问该网站时所进行的操作，用户可以根据需要在下拉列表中选择“允许”或“拒绝”选项。若选中“启用域名限制”复选框，即可启用域名限制。需要注意的是，通过域名限制访问会要求 DNS 反向查找每一个连接，这将会严重影响服务器的性能，建议不要使用。

05 在“操作”栏中单击“恢复为继承的项”链接，显示如图 14.21 所示“IPv4 地址和域限制”对话框，恢复功能以从父配置中继承设置，该操作将为当前功能删除本地配置设置（包括列表中的项目），应慎重使用。



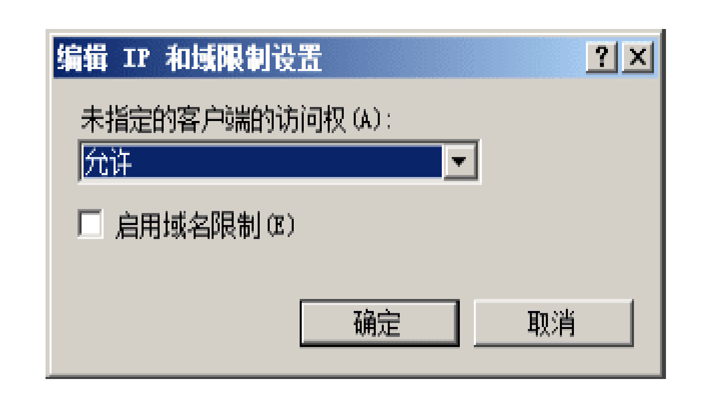


图 14.20 “编辑 IP 和域限制设置”对话框

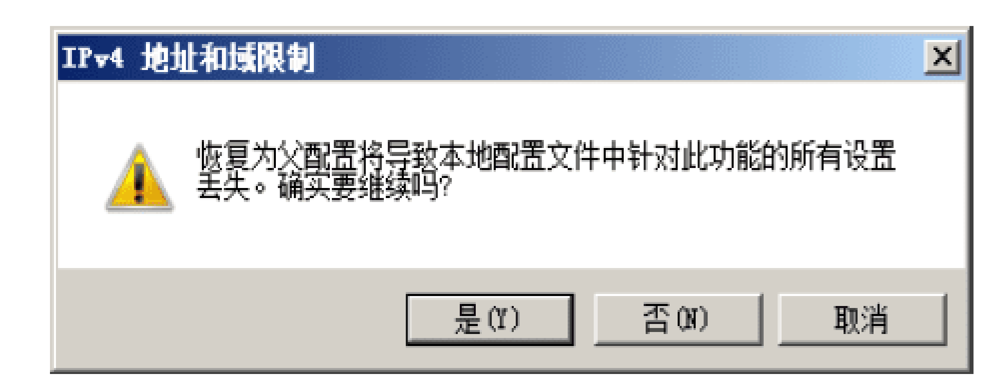


图 14.21 “IPv4 地址和域限制”对话框

06 在“操作”栏中单击“查看经过排序的列表”链接，显示如图 14.22 所示窗口。IIS 7.0 是按照限制规则列表中条目的顺序依次执行的。例如，当前规则列表中包括两条限制条目：拒绝 IP 地址为 192.168.1.21 的主机访问，允许整个 192.168.1.1～192.168.1.254 网段访问，即被拒绝的 IP 地址 192.168.1.21 又在被允许访问的网段内。此时，如果经过排序后拒绝在先，将拒绝指定用户访问；如果允许在先则将允许该用户访问。



图 14.22 查看经过排序的列表

07 在经过排序的限制列表中，选择想要移动的限制条目，单击“上移”或“下移”链接，即可调整执行顺序。

14.4.5 内容分级设置

IIS 7.0 中的托管模块设计为管理员的工作提供了极大的便利。.NET 信任级别功能可以托管模块、处理程序和应用程序指定信任的级别。通过用户组可以对一组用户进行分类，并对定义的用户组执行与安全相关的操作。需要注意的是，设置信任级别之前，必须先在“.NET 用户”窗口中，添加相关的用户角色，该功能需要 SQL Server 2005 数据库的支持。

01 在“Internet 信息服务管理器”窗口的站点（以 Default Web site 站点为例）主页中，双击“.NET 信任级别”图标，显示如图 14.23 所示“.NET 信任级别”窗口。

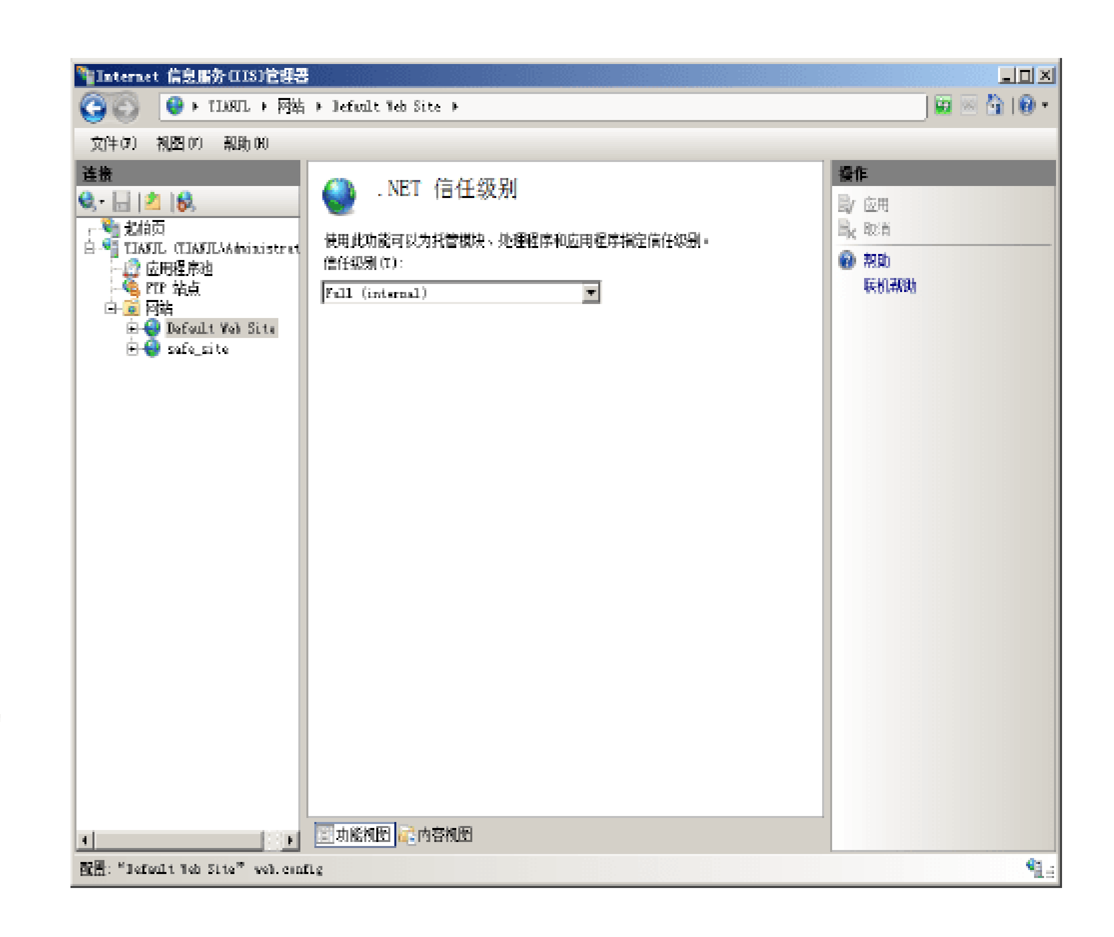


图 14.23 “NET 信任级别”窗口

02 在“信任级别”下拉列表中，选择适当的信任级别即可，系统默认为“Full（internal）”级别。各个信任级别的具体含义如下：

- Full（internal）级别。指定不受限制的权限。授予 ASP.NET 应用程序权限，以便允许访问任何符合操作系统安全性的资源，支持所有特许操作。该信任级别是用于内部网络的 Web 站点，安全性最低；
- High（web_hightrust.config）。指定高级别的代码访问安全性，表示在默认情况下，应用程序无法执行下面任何一项操作：
  - 调用非托管代码；
  - 调用服务组件；
  - 向事件日志中写入内容；
  - 访问消息队列服务队列；
  - 访问 ODBC、OleDb 或 Oracle 数据源。
- Medium（web_mediumtrust.config）。指定中等级别的代码访问安全性，即默认情况下，除了高信任级别的限制以外，ASP.NET 应用程序还无法执行下面任何一项操作：
  - 访问应用程序目录范围之外的文件；
  - 访问注册表；
  - 进行网络或 Web 服务调用。
- Low（web_lowtrust.config）。指定低级别的代码访问安全性，表示在默认情况下，除了中等信任级别的限制以外，该应用程序还无法执行下面任何一项操作：
  - 向文件系统中写入内容；
  - 调用 Assert 方法。
- Minimal（web_minimaltrust.config）。指定最低级别的代码访问安全性，这表明该应用程序只具有执行权限，安全级别最高。

03 在“操作”栏中，单击“应用”链接，保存设置即可。

14.5 使用 SSL 证书配置安全 Web 站点

除通过上述基本措施确保 Web 服务器安全之外，管理员还可以使用 SSL 证书搭建安全 Web 站点。随着电子商务网络应用的日益推广，SSL 安全协议的使用得非常广泛，目前的 V3.0 版本已经成为一个国际标准，并得到了所有浏览器和服务器软件的支持。在 Windows Server 2008 系统的 IIS 7.0 中，可以通过自签名证书或来自 CA 的证书搭建安全 Web 站点。

14.5.1 SSL 安全协议概述

SSL（Secure Socket Layer）协议是 Netscape 公司研发的一个可以保障用户在 Internet 上传



输数据的安全，确保在网络上传输的数据不被截取和窃听的安全协议。SSL 协议提供的主要服务有：

- 认证用户和服务器，确保数据发送到正确的客户机和服务器上；
- 加密数据防止数据被截取；
- 维护数据的完整性，确保数据在传输过程中不被改变。

SSL 协议使用不对称加密技术来实现双方之间信息的安全传递。不同于常用的 HTTP 协议，客户端与 SSL 安全网站连接时使用的是 https 协议，即采用 https://*的方式来访问。

HTTPS（Secure Hypertext Transfer Protocol）安全超文本传输协议，是以安全为目标的 HTTP 通道，它默认使用 443 端口进行通信，应用 SSL 作为应用层的子层，适用于商业信息的加密。

14.5.2　申请服务器证书

搭建 SSL 证书加密的安全 Web 站点之前，必须先获得服务器证书。如果网络中没有部署证书服务器，可以在 IIS 服务器上创建自签名服务器证书，当然也可以像域中的域控制器申请服务器证书。如果使用独立证书颁发机构，那么用户提交证书申请后，需要以管理员身份登录到证书服务器，手动颁发所需证书。如果网络中没有部署任何 CA，可以使用自动签名证书功能。

01 在“Internet 信息服务管理器”窗口中，打开“WIN-HKSLEYF2NMT（服务器名）主页”，双击“服务器证书”图标，显示如图 14.24 所示“服务器证书”窗口。

02 单击“创建域证书”选项，显示如图 14.25 所示“可分辨名称属性”窗口。在“通用名称”文本框中输入申请证书的计算机名称，如果是为 Web 服务器申请证书，输入 Web 服务器的域名或 IP 地址，其他根据实际需要填写即可。

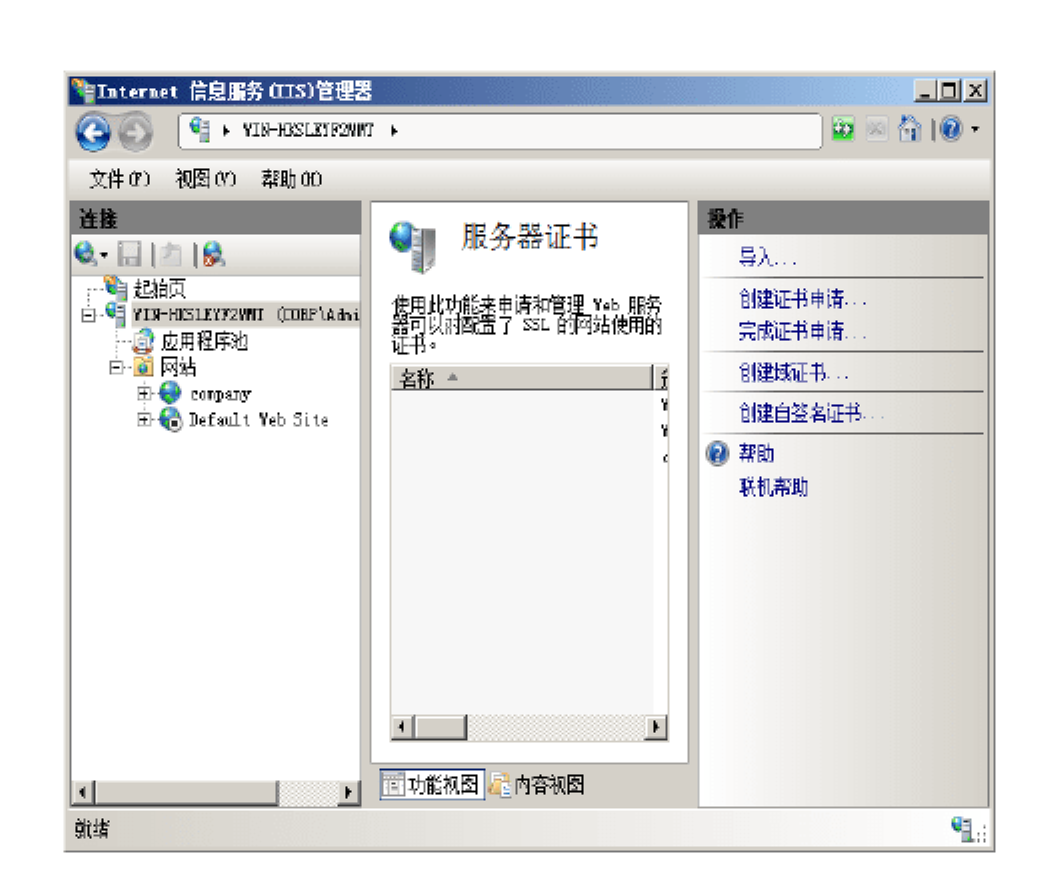


图 14.24　“服务器证书”窗口

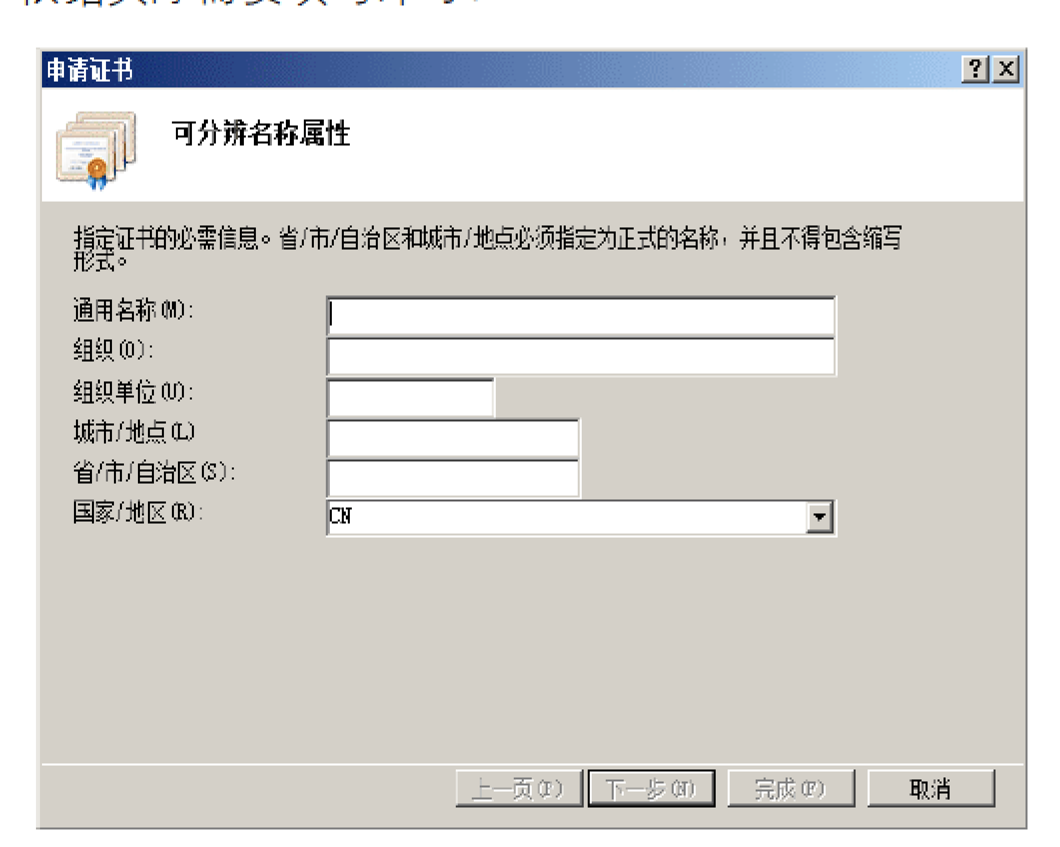


图 14.25　“可分辨名称属性”窗口

03 单击“下一步”按钮，显示“联机证书颁发机构”对话框。单击“选择”按钮，打开如图 14.26 所示“选择证书颁发机构”对话框，选择该证书，单击“确定”按钮，返回“选择证书颁发机构”窗口，在“好记名称”文本框中，输入便于识别的证书名称即可。

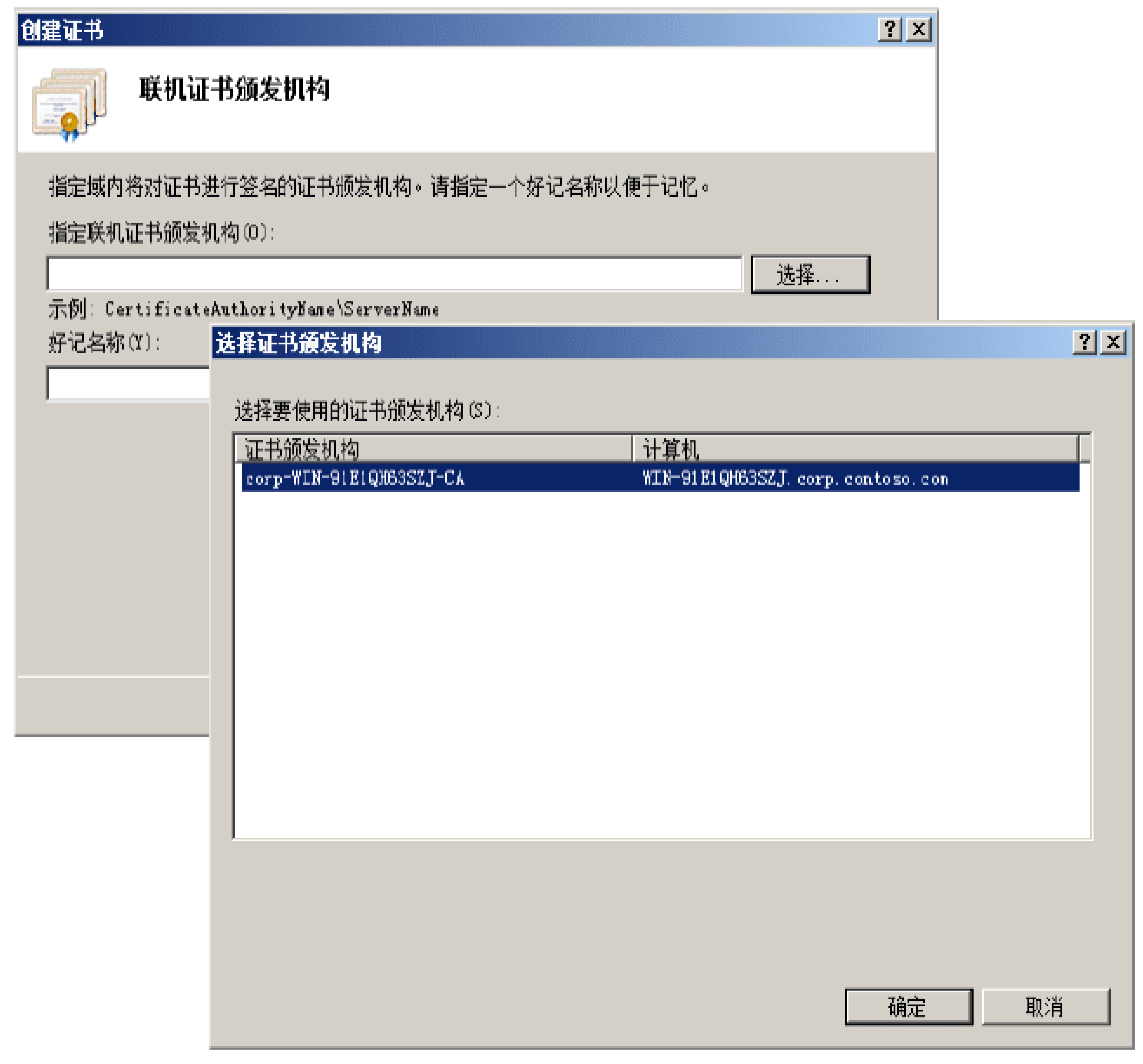
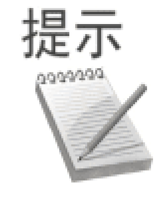


图 14.26　选择证书颁发机构

04 单击“完成”按钮，完成证书申请。



提示　使用企业证书颁发机构申请证书后，服务器可以立即为用户颁发所需证书。登录证书服务器，依次选择“开始”→“管理工具”→“Certification Authority”命令，打开“证书颁发机构”对话框，即可查看颁发给 Web 服务器的证书。

14.5.3　创建 HTTPS 安全站点

SSL 证书只能应用于启用安全设置的 Web 站点，即 HTTPS 站点。获得应用于安全站点的服务器证书后，即可开始创建安全站点，并将 SSL 证书和 Web 站点绑定。需要注意的是，HTTPS 站点只能在创建 SSL 证书后创建，不能将已创建的 HTTP 站点更改为 HTTPS 站点。

01 选择“开始”→“管理工具”→“Internet 信息服务管理器”命令，在“连接”栏中，右击“网站”链接，在弹出的快捷菜单中选择“添加网站”选项，显示如图 14.27 所示“添加网站”对话框，在“网站名称”文本框中输入网站名称，在“物理路径”文本框中输入网站的物理路径，“类型”下拉列表框中选择“https”,“IP 地址”和“端口”使用默认设置即可，在“SSL 证书”下拉列表中，选择所创建的域证书。单击“确定”按钮，完成 HTTPS 网站创建。

02 在 IIS 管理器窗口中，单击新建的 HTTPS 网站显示其主页，双击“SSL 设置”图标，显示如图 14.28 所示“SSL 设置”窗口。选中“要求 SSL”复选框，可以选择“需要 128 位 SSL”复选框的加密算法。客户证书的接受方式有 3 项：

- 忽略：不要求客户端在获得内容访问权限之前验证身份，安全性最低；
- 接受：如果要接受客户端证书，并在允许客户端获得内容访问权限之前验证客户端身份，则选择该设置；



■ 必需:在允许客户端获得内容访问权限之前要求证书验证客户端省份。

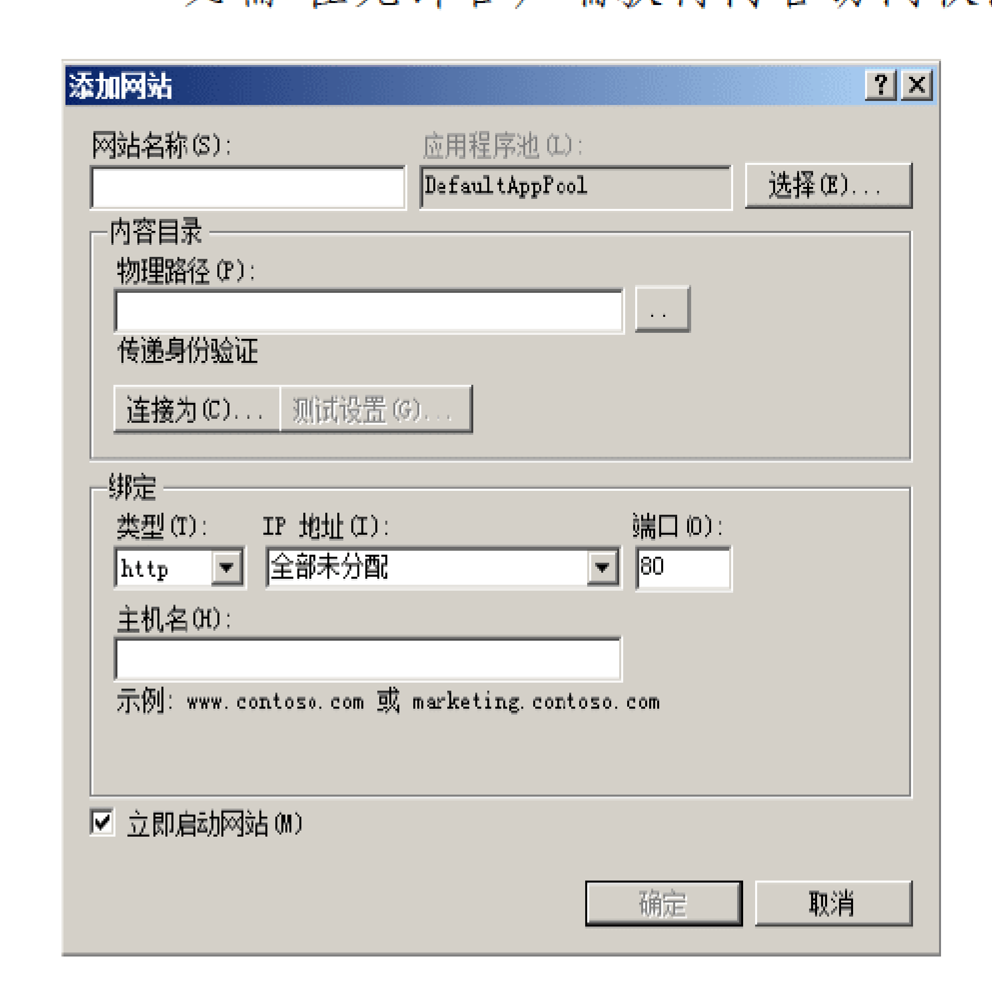


图 14.27　“添加网站”对话框



图 14.28　“SSL 设置”窗口

03 设置完后，在“操作”栏中单击“应用”选项，完成设置。

14.5.4　浏览 HTTPS 网站

由于 HTTPS 网站，采用了 SSL 安全设置，这要求访问该服务器网站的客户端必须提供有效的数字证书。管理员可以将 Web 服务器上使用的 SSL 证书导出为文件，然后发布到客户端并导入到受信任的根证书颁发机构。

01 登录到 Web 服务器，在 IIS 管理器中选择 Web 服务器名称，双击“服务器证书”，打开“服务器证书”窗口。选择安全站点使用的 SSL 证书，右击并选择快捷菜单中的“导出”选项，显示如图 14.29 所示“导出证书”对话框。单击“浏览”按钮，选择证书的保存路径，并设置证书文件名，或者在“导出至”文本框中直接输入。在“密码”和“确认密码”文本框中，设置一个密码。单击“确定”按钮即可将证书导出。导出后的证书是一个扩展名为.pfx 的文件。

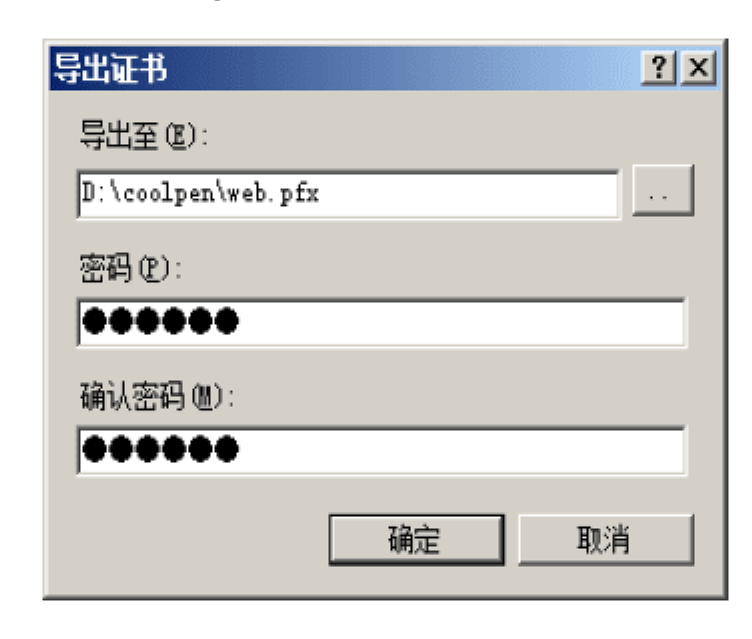


图 14.29　“导出证书”对话框

02 通过某种方式，将该证书发布给客户端用户。在客户端计算机上，双击证书文件，启动“证书导入向导”。依次单击“下一步”按钮，选择要导入的证书文件和输入导入密码，如图 14.30 所示。在“密码”文本框中输入导出证书时设置的密码即可。

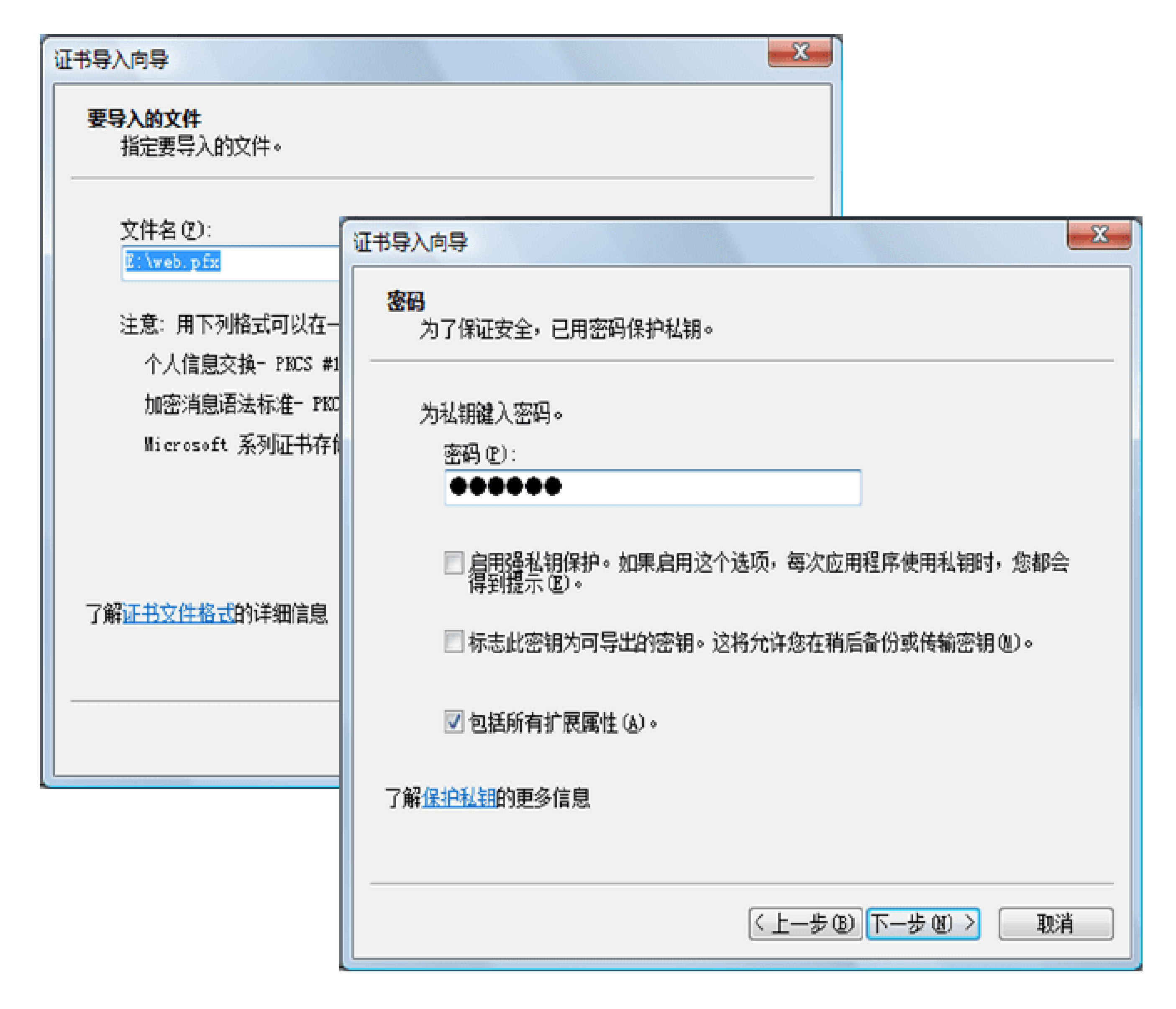


图 14.30　选择要导入的证书和密码

03 单击“下一步”按钮，显示“证书存储”对话框。选择“将所有的证书放入下列存储”单选按钮，单击“浏览”按钮，显示如图 14.31 所示“选择证书存储”对话框。选择“受信任的根证书颁发机构”选项，并单击“确定”按钮。

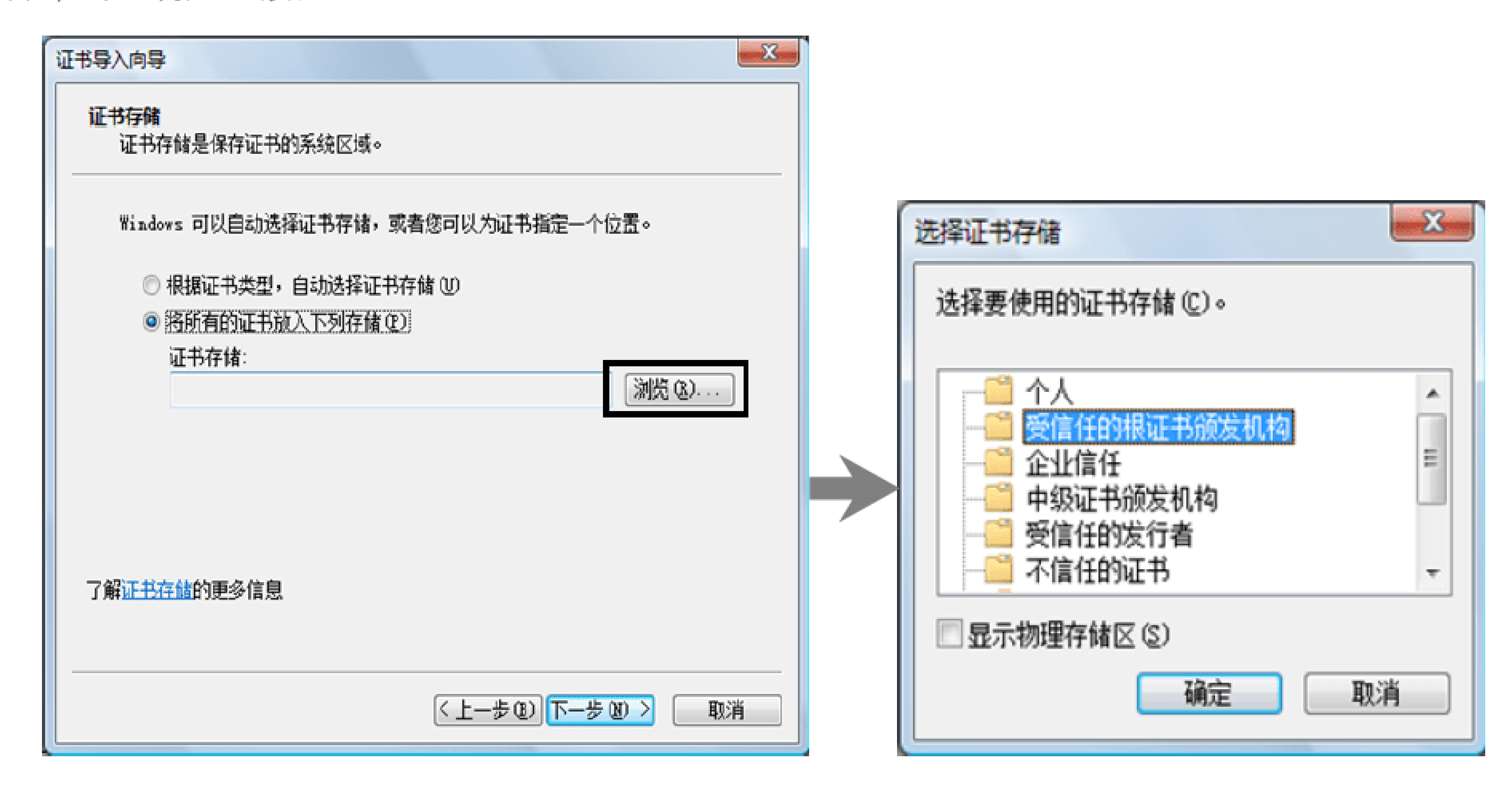


图 14.31　选择证书存储

04 单击“下一步”按钮，显示“正在完成证书导入向导”对话框。单击“完成”按钮，显示如图 14.32 所示“安全性警告”对话框。要求确认是否信任该证书颁发机构。单击“是”按钮，即可将该证书导入本地计算机。

05 打开 IE 浏览器，在地址栏中输入网站地址，格式为：https://Web 服务器名，回车，显示如图 14.33 所示“选择数字证书”对话框。



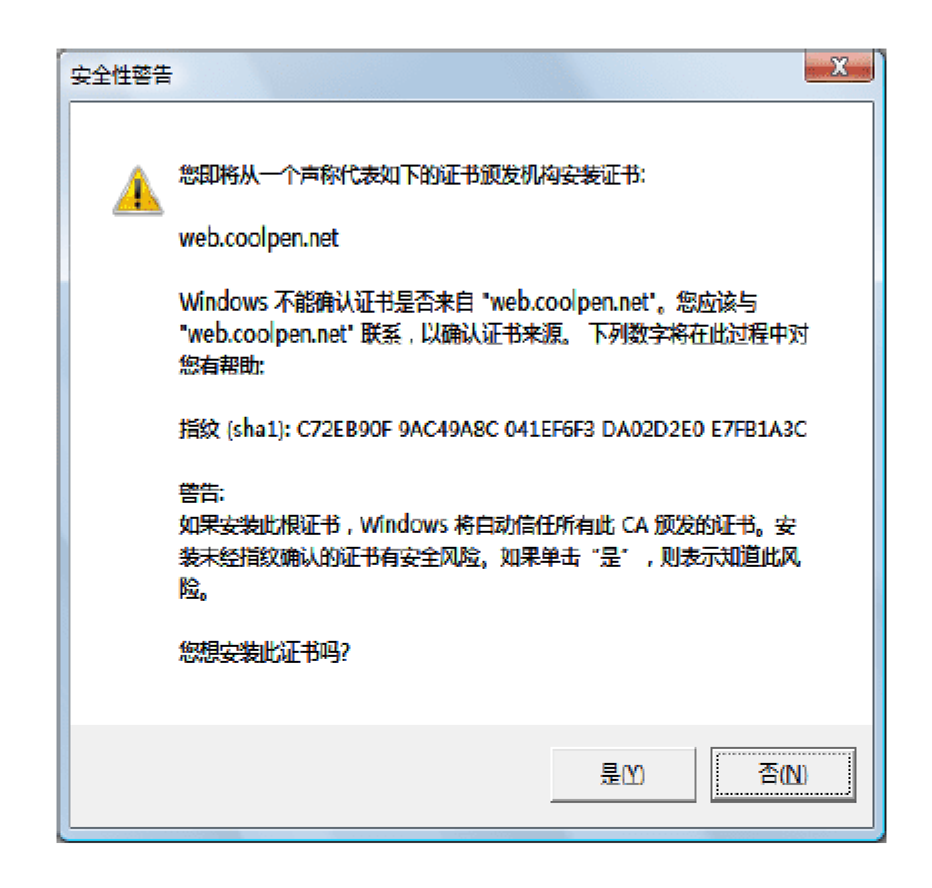


图 14.32　“安全性警告”对话框

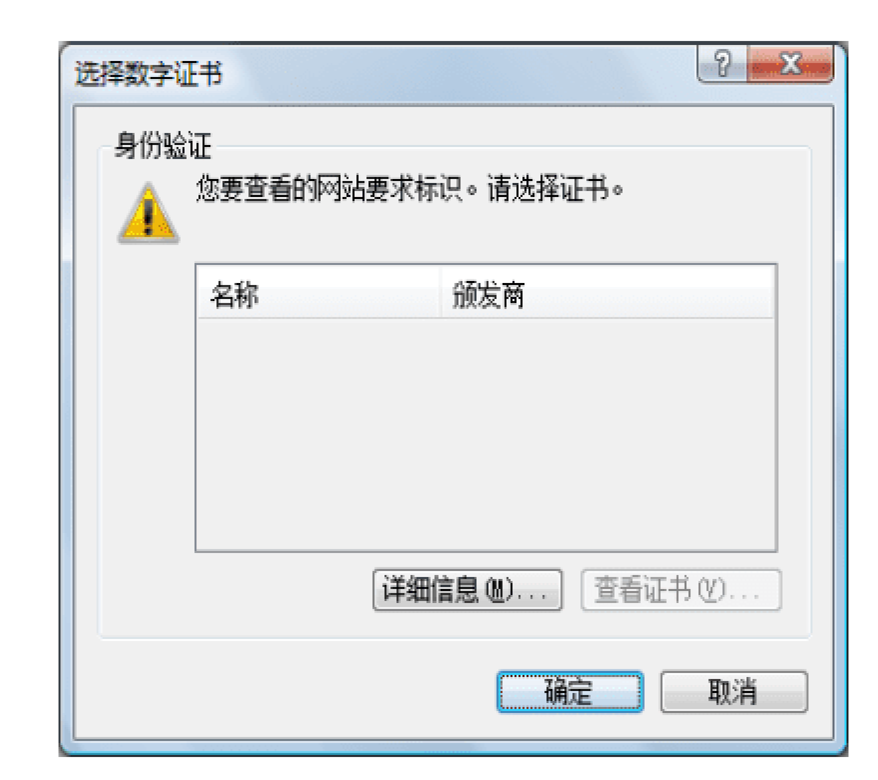


图 14.33　“选择数字证书”对话框

06 单击“确定”按钮，即可打开该网站。在地址栏右侧会显示一个锁形标识，如图 14.34 所示。表示当前正在使用证书进行加密传输。

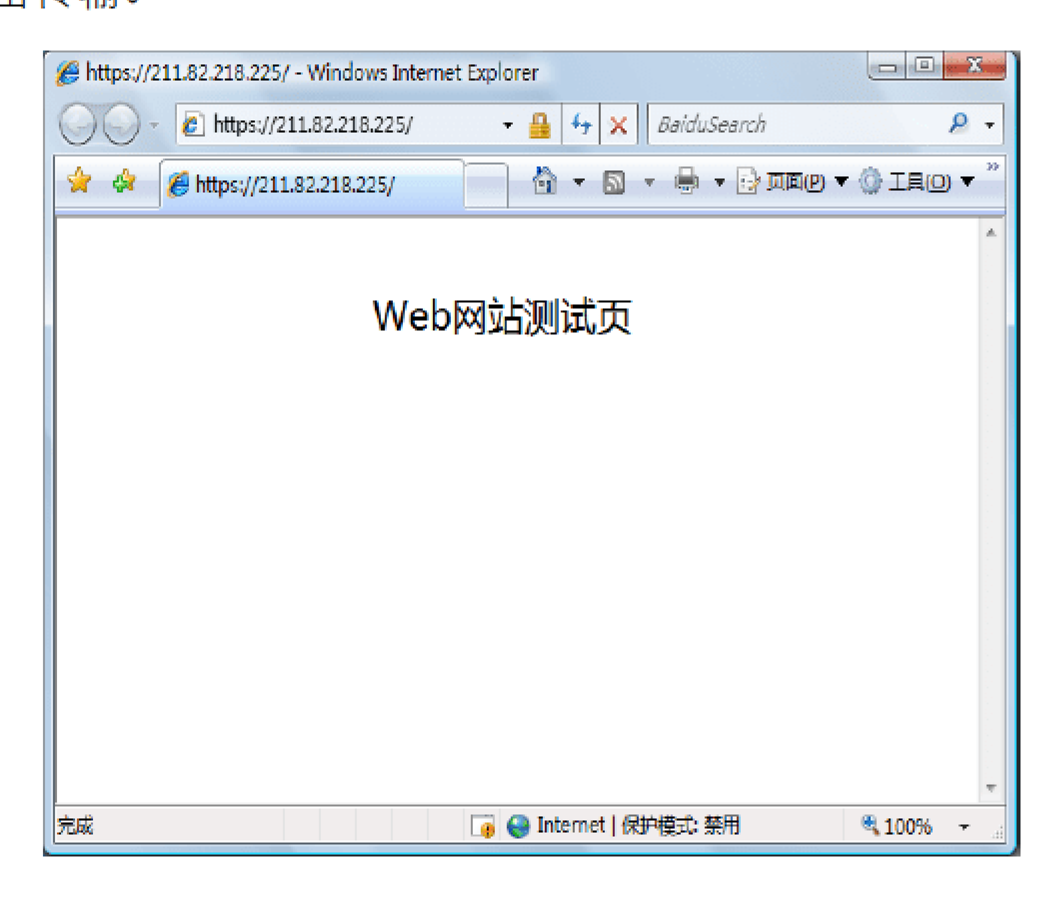


图 14.34　使用证书传输

提示　浏览 Web 安全网站需要客户端浏览器对 SSL 协议的支持，否则将无法打开经过 SSL 加密的安全站点。可以在 IE 浏览器窗口中选择“工具”→“Internet 选项”→“高级”命令中查看。

14.5.5　SSL 证书安全漏洞及防范措施

1. SSL 证书安全漏洞

由于传统的防火墙和网关反病毒方案并不能扫描到加密通信，因此也就不能控制那些通过 HTTPS 进入和流出网络的内容。SSL 常见的安全问题有下面三种。

（1）攻击证书

随着 SSL 安全技术的广泛应用，第三方认证机构也不断涌现。很多 Web 网站都向认证机构申请安全证书，过于信任公共 CA 机构，将会隐藏巨大的安全。IIS 7.0 服务器提供的“客户

端证书映射”功能，用于将客户端提交证书中的名字映射到系统用户帐户。这种情况下，访问者将可以获取该系统管理员的特权。

暴力攻击证书是一种常用且有效的攻击，它只需猜测一个有效的用户名，而不用猜测用户名和密码。首先入侵者编辑一个可能的用户名列表，用这些用户向 CA 机构申请证书。其中每个证书都用于尝试获取访问权限。用户名越多，其中一个证书被认可的可能性也就越高。

（2）窃取证书

证书有一个致命的弱点，那就是私钥。私钥往往被放在本地计算机上，这很容易被入侵者利用特洛伊木马获取。所以应将证书保存在移动存储设备中，与计算机脱离，当需要的时候再连接。

（3）安全盲点

由于 HTTPS 是加密通信，安全扫描软件只能查找普通 Web 站点的安全盲点，却无法检查经过 SSL 保护的服务器。

2. 安全防范措施

尽管采用 SSL 协议的 Web 站点可能存在各种漏洞，但相对而言其安全性还是比普通 Web 站点要高很多。所以对安全性较高的站点应尽量采用 SSL 证书加密。同时还可以采用第三方软件对 Web 安全站点进行安全防护。

（1）安全 ISA 防火墙

微软于 2008 年 4 月 8 日发布了 ISA Server 新一代版本 Forefront TMG 的测试版，和以往 ISA 相比，TMG 具有划时代的企业安全产品。主要功能如下：

- 企业级的整合与管理；
- 架构变更与提升；
- Web 反病毒与过滤；
- 人性化管理与集成操作。

（2）Web 安全服务器

入侵检测只能检测纯文本的数据内容，若想检测 SSL 安全站点的通信记录，可以检测服务器上的 SSL 连接，或者将连接上的数据转换为纯文本格式。一般网站都会开启基本的日志记录功能。例如 IIS 内置的日志功能，可以检查到很多一般网站的入侵事件。

14.6 FTP 服务安全

FTP 服务器的主要功能是提供文件上传和下载，可以帮助用户实现软件的下载、文件的交换与共享、以及 Web 站点的维护等。由于 FTP 以明文形式传送信息，所以很容易被其他用户



截获。因此，对基于 IIS 的 FTP 服务器必须实施相关安全措施。安装 IIS 7.0 过程中，默认没有安装 FTP 服务，用户需要手动添加。FTP 服务管理仍然采用 IIS 6.0 管理控制台，因此必须同时安装“IIS 6.0 管理兼容性”组件。

14.6.1　禁止匿名访问

默认情况下，在 IIS 上架构的 FTP 站点，用户都可以用 IUSR_SERVERNAME 帐户连接该 FTP 服务器，使用 anonymous 帐户，密码可以使用任何内容，就能匿名登录 FTP 站点。

01 在“Internet 信息服务 6.0 管理器”窗口中，依次展开“WIN-HKSLEYF2MMT”→“FTP 站点”选项，右击 FTP 站点（以 Default FTP Site 为例），选择快捷菜单中的“属性”命令，显示“Default FTP Site 属性”对话框。切换至“安全帐户”选项卡，取消“允许匿名连接”复选框，显示如图 14.35 所示“IIS6 管理器”对话框。

02 单击“是”按钮，关闭“IIS6 管理器”对话框。在“安全帐户”选项卡中，单击“确定”按钮，即可禁止用户匿名访问该 FTP 站点，如图 14.36 所示。

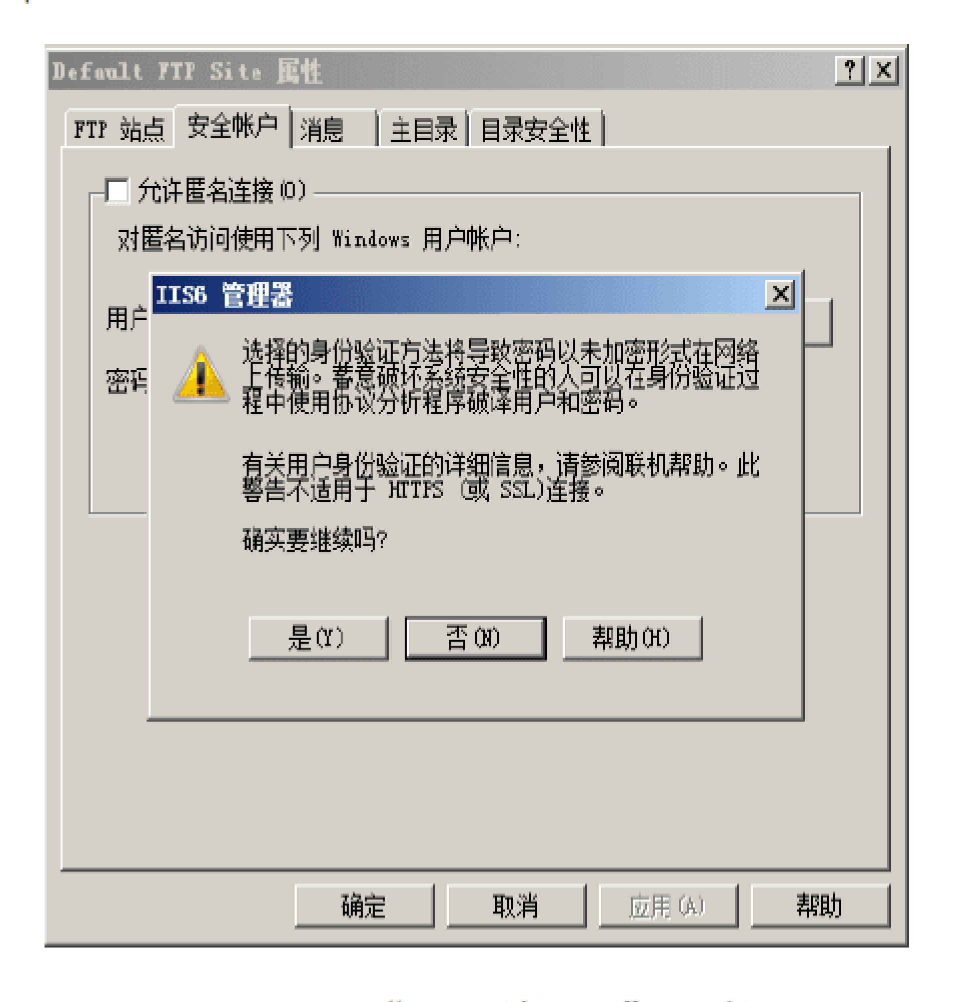


图 14.35　“IIS6 管理器”对话框

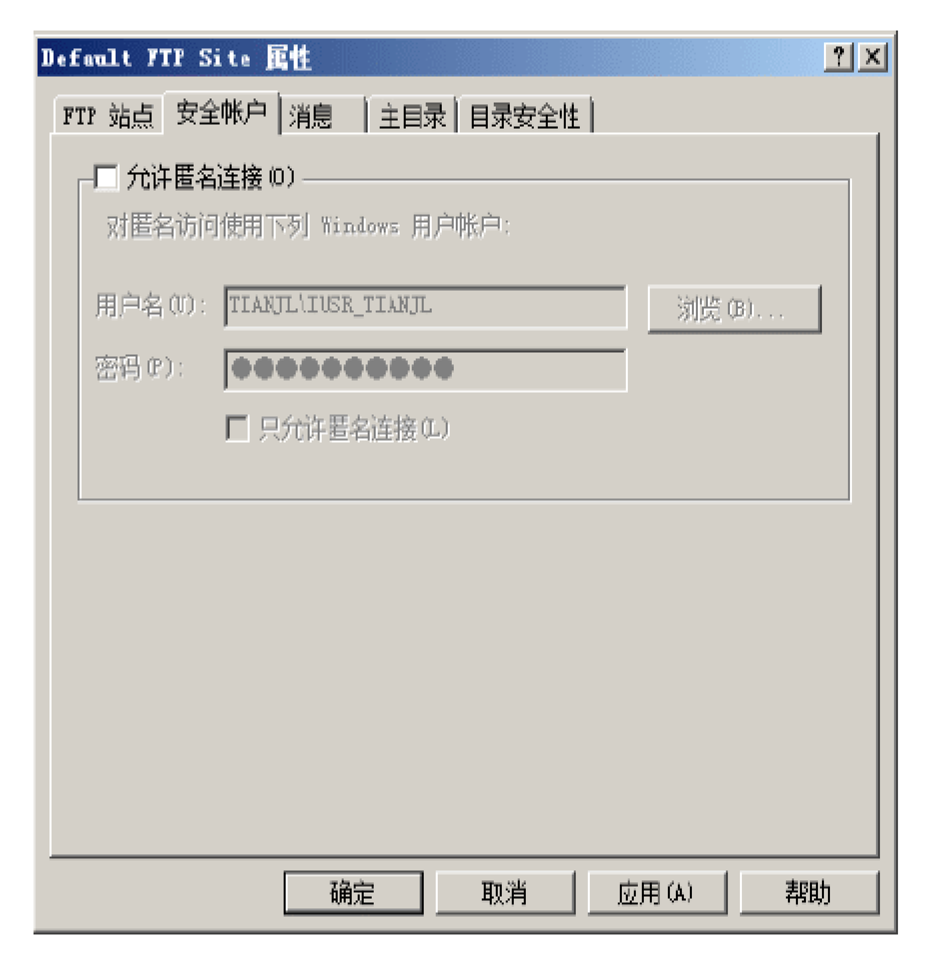


图 14.36　“安全帐户”选项卡

当禁止用户匿名连接后，只有服务器或活动目录中有效的帐户，才能通过身份认证，并实现对该 FTP 站点的访问。

除禁止匿名连接外，还可以在本地计算机或域控制器上，创建专用于 FTP 连接的匿名用户帐户（区别于系统默认的 IUSR_服务器名帐户），对其在 FTP 主目录或单个文件夹的权限进行限制，实现 FTP 服务器的安全。选中“允许匿名连接”复选框，单击“浏览”按钮，选择指定用户帐户即可。单击“应用”按钮，系统将自动添加对应帐户的密码，如图 14.37 所示。如果选择“允许匿

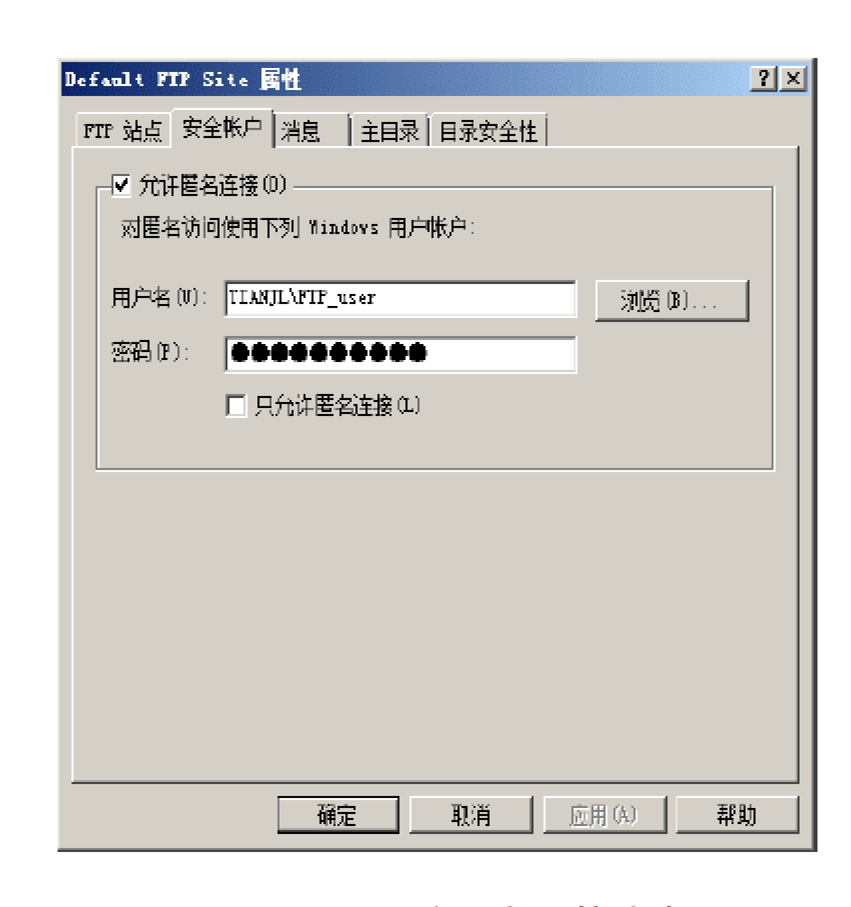


图 14.37　更改匿名连接帐户

名连接”复选框，用户将无法使用用户名和密码登录 FTP 服务器。此选项拒绝访问使用具有管理凭据帐户的那些用户，而只为使用匿名访问帐户的用户指派访问权限。

14.6.2　TCP 端口和连接数设置

FTP 默认的端口号是 21，恶意用户可以用扫描器探测到该服务器已经开放了 FTP 且如果站点连接为不受限制的话，恶意用户可以无数次连接该服务器的 21 端口，导致服务器的 CPU 和内存资源使用率达到 100%，使其无法正常运行。

在“Internet 信息服务 6.0 管理器”窗口中，右击“Default FTP Site”选项，在弹出的快捷菜单中选择“属性”命令，打开“Default FTP Site 属性”对话框。默认显示如图 14.38 所示“FTP 站点”选项卡，在“TCP 端口”文本框中输入未被占用的其他端口号，选中“连接数限制为”单选按钮，根据实际情况在“连接数限制为”文本框中输入限制连接数，在“连接超时”文本框中输入超时时间。

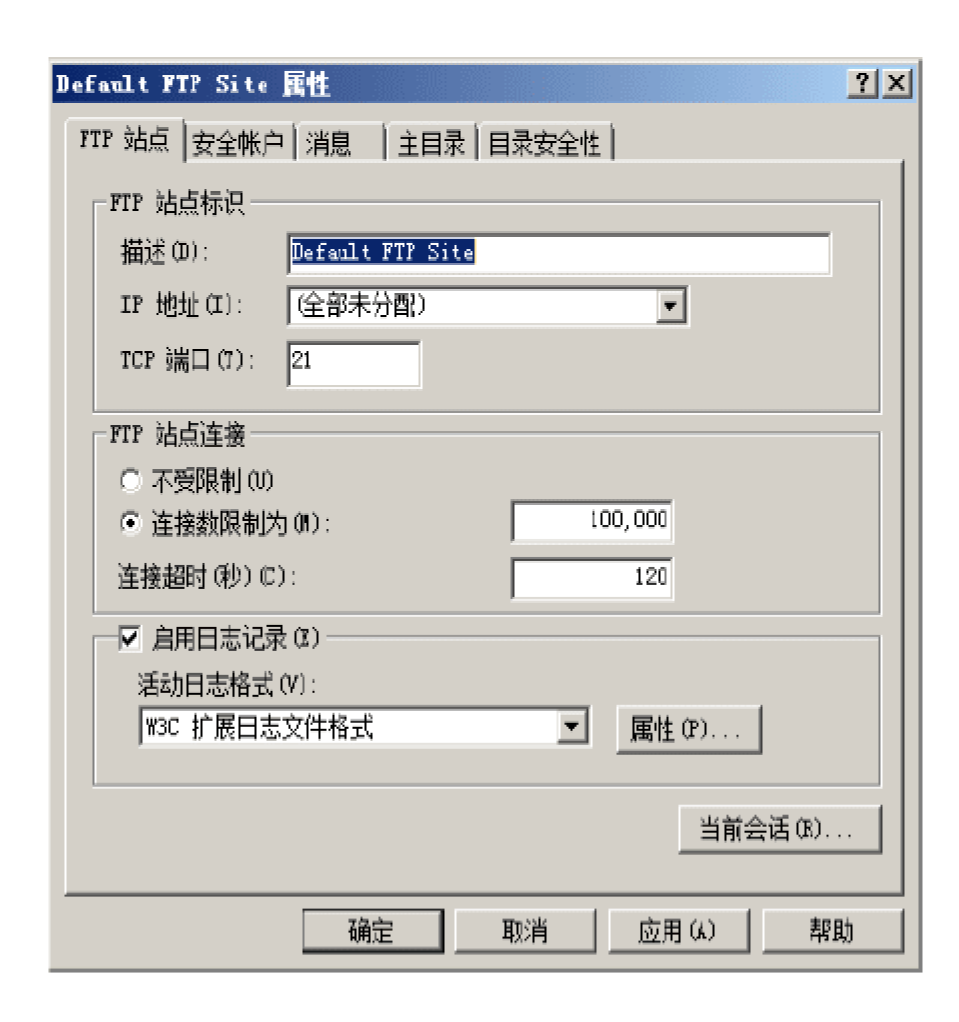
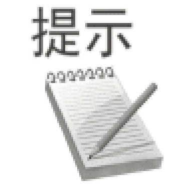


图 14.38　“Default FTP Site 属性”对话框



提示　在命令提示符窗口中通过“netstat-a”命令查看已经使用了哪些端口。更改端口后，要访问该 FTP 站点必须指定端口号。默认已经启用了日志记录，管理员可以单击“属性”按钮来设置日志记录属性，如图 14.39 所示。

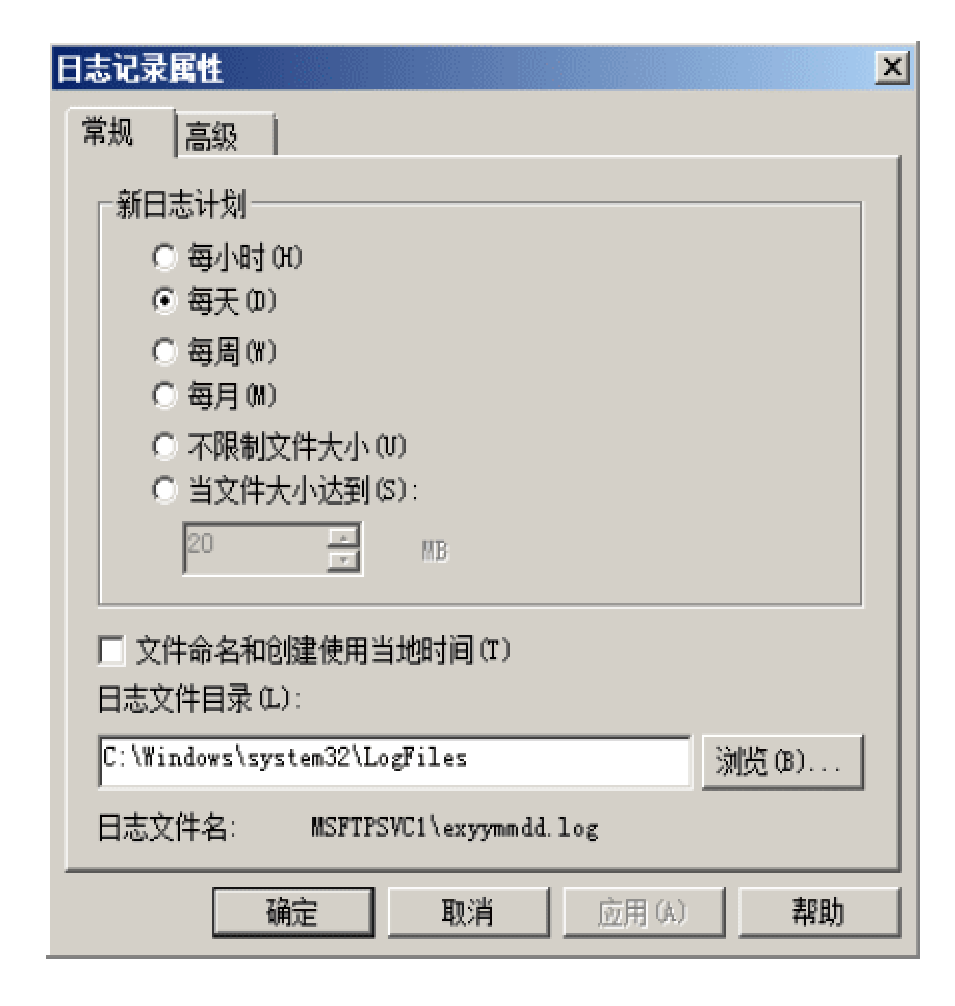


图 14.39　“日志记录属性”窗口

14.6.3　TCP/IP 地址访问限制设置

通过对 IP 地址的限制，可以只允许或拒绝某些特定范围内的计算机访问该 FTP 站点，从而可以在很大程度上避免来自外界的恶意攻击，并且将授权用户限制在某一个范围。将 IP 地址限制与用户认证访问结合在一起，将进一步提高 FTP 站点访问的安全性。特别是对于企业内部的 FTP 站点而言，采用 IP 地址限制的方式，是非常简单而有效的。



01 打开 FTP 站点属性对话框，切换到“目录安全性”选项卡，选择“拒绝访问”单选按钮，表示默认情况下所有计算机均被拒绝访问，只有将要添加的 IP 地址用户可以访问。相反，也可以设置为默认情况下所有计算机都将被“允许访问”，然后创建需要拒绝访问的 IP 地址列表。单击“添加”按钮，显示如图 14.40 所示“授权访问”对话框，默认选择“一台计算机”单选按钮，每次只能添加一个 IP 地址。建议选择“一组计算机”单选按钮，在“网络标识”和“子网掩码”文本框中，输入相应的网络标识信息，添加一个网段内的所有 IP 地址。

02 单击“确定”按钮，将该所选 IP 地址或 IP 地址段添加至“下列除外”列表中，如图 14.41 所示。创建“拒绝访问”IP 地址列表的方法与之相同，此处不复赘述。

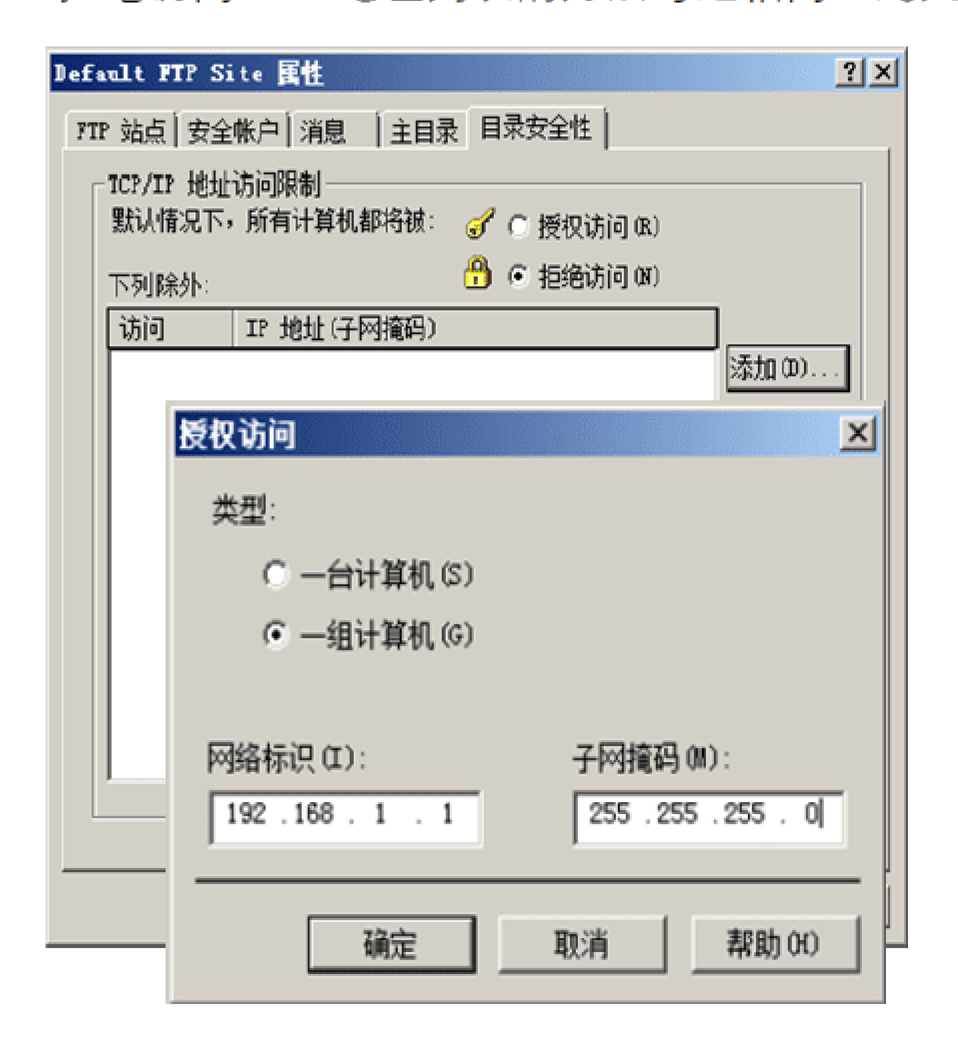


图 14.40　“授权访问”对话框

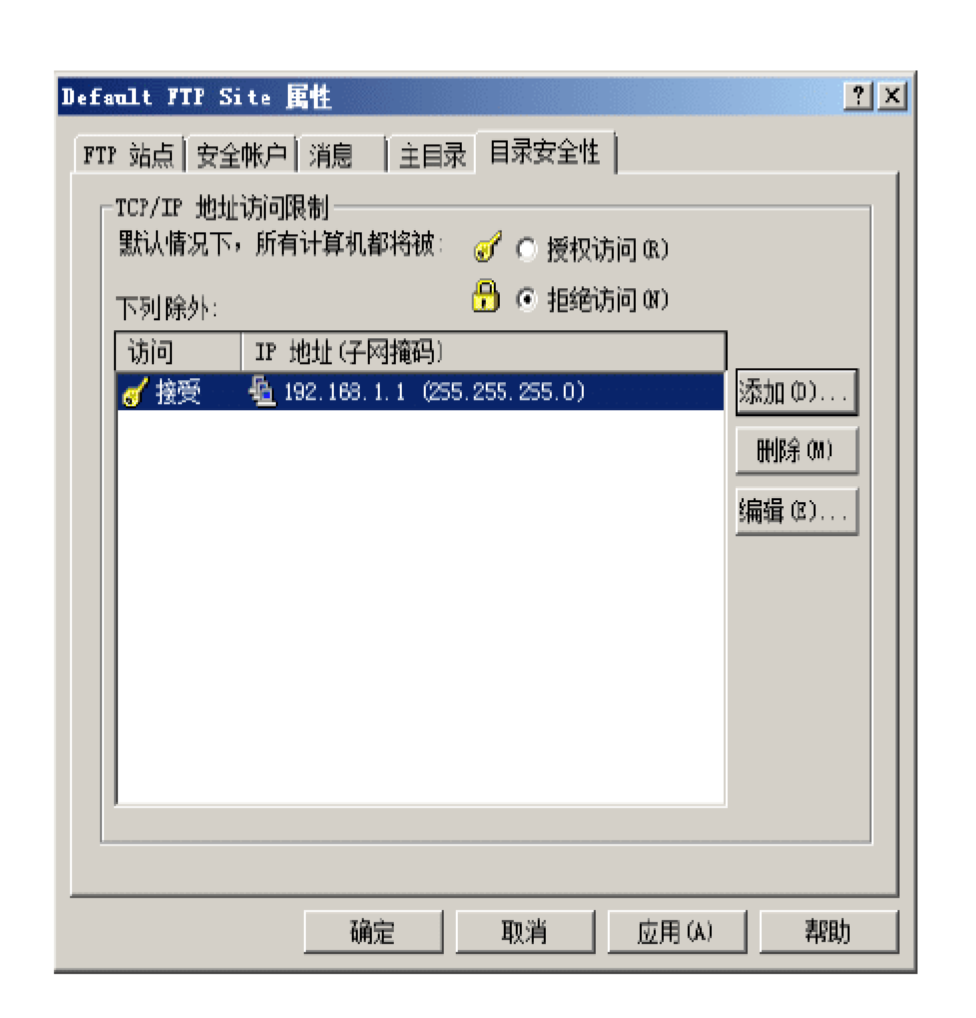


图 14.41　创建成功的授权访问 IP 地址

03 单击“确定”按钮，保存设置即可。

14.6.4　设置 NTFS 访问权限

默认情况下，在 FTP 服务器上只能为文件设置简单的“读取”和“写入”权限，并且默认本地服务器或域中所有的用户都具有访问权限。有时需要为用户设置更详细的权限，这就要借助于 NTFS 权限来实现。通常，将 FTP 服务器与 NTFS 权限相结合，和文件服务器一样，为 FTP 站点中的文件设置多种不同的权限，以满足不同用户的使用。

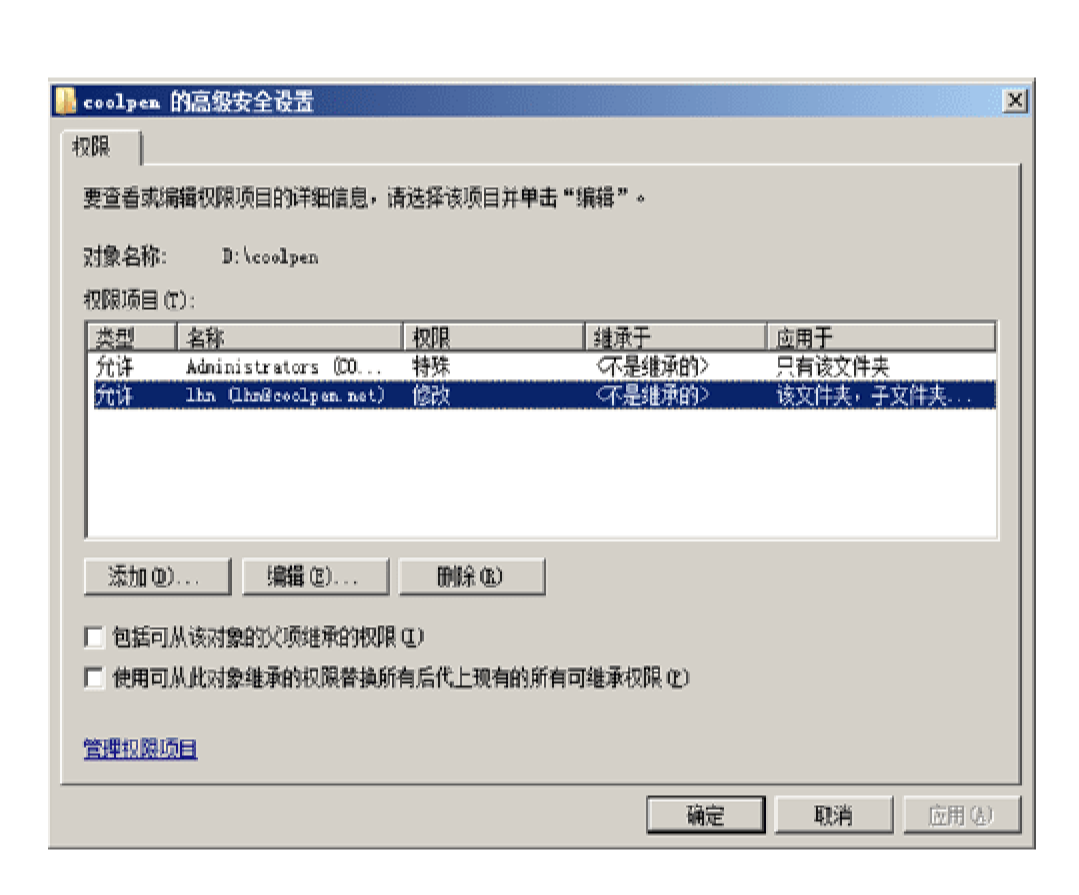
01 在“文件夹属性”对话框的“安全”选项卡中，单击“编辑”按钮，显示“coolpen 的权限”对话框，默认只保留了 Administrators 用户组。单击“添加”按钮，显示如图 14.42 所示“选择用户、计算机或组”对话框，在“输入对象名称来选择”文本框中输入将要分配读写权限的用户，例如 lhn，或者单击“高级”按钮查找。

02 单击“添加”按钮，即可添加该用户并返回权限对话框，选择新添加的用户，在权限列表中即可选择将要分配的权限，共有 6 种权限可供选择，分别是：完全控制、修改、读取和执行、列出文件夹目录、读取和写入。单击“确定”按钮保存并返回“安全”选项卡。



图 14.42　添加希望设置 NTFS 权限的用户或组

03 如果要为该用户分配更详细的权限，可在“安全”选项卡中单击“高级”按钮，显示“coolpen 的高级安全设置”对话框，单击“编辑”按钮，在“权限项目”列表框中选择欲设置的用户帐户，单击“编辑”按钮，显示如图 14.43 所示“coolpen 的权限项目”对话框，在“权限”列表框中可以选择更详细的权限，共有 14 种权限可供选择。



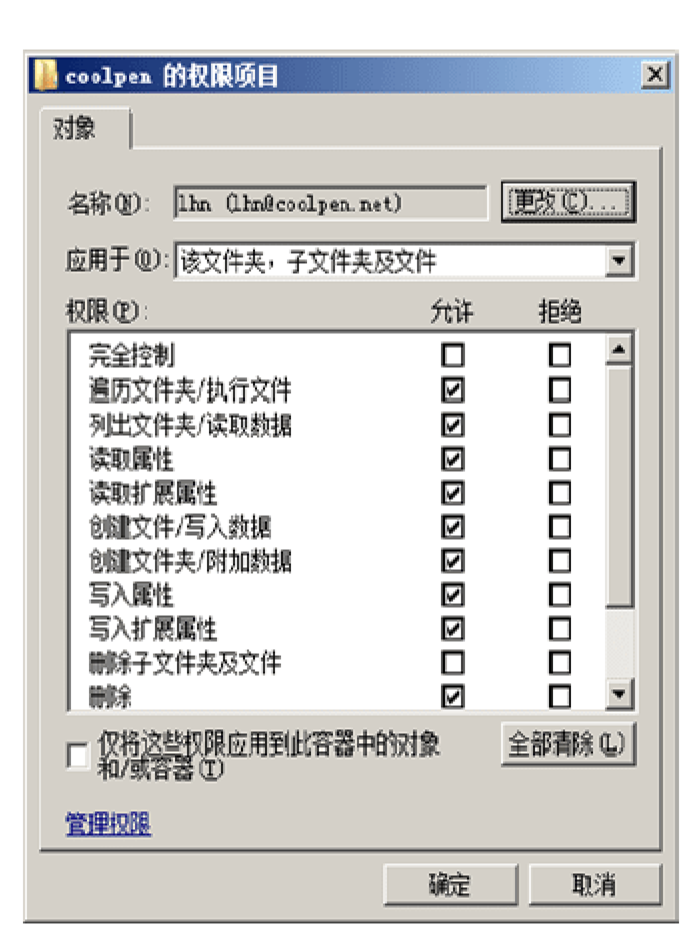


图 14.43　更改高级安全设置

04 选择完成后，依次单击“确定”按钮保存即可。

利用这种方式设置的用户权限更加详细，可以精确到是否允许用户读取、删除、删除子文件夹及文件、创建文件或文件夹等，从而可以更好地控制用户对 FTP 文件夹的访问。

14.6.5　使用磁盘配额限制可用空间

默认情况下，FTP 服务器并不限制用户上传文件的总大小，因此，当为 FTP 用户赋予了写入权限时，用户就可以向 FTP 服务器中上传任意大小的文件，从而导致服务器中宝贵的硬盘空间被迅速占用。为了保护硬盘空间，应当启用磁盘配额功能，来限制每个用户使用磁盘空间的大小。

FTP 服务器本身并没有提供磁盘限额功能，需要借助 Windows Server 2008 系统中的 NTFS 文件



系统来实现。因此，FTP 主目录必须位于 NTFS 格式的分区，FAT32 文件系统无法设置磁盘配额。

为用户设置了磁盘配额以后，当用户上传的文件超出空间限制或者到警告等级时，系统将自动发出警告，提示用户超出空间配额，上传操作不能完成等信息。关于磁盘配额的设置，请参见本书中的相关内容，这里不再赘述。

小　　结

Web 和 FTP 是网络中应用最广的网络服务。Windows Server 2008 系统集成的 IIS 7.0 组件，无论是安全性还是可管理性，都有了很大的提高，允许管理员通过多种安全机制，保护服务器和访问连接的安全。在 Web 服务器安全管理中，管理员可以设置 NTFS 访问权限、身份验证、IPv4 地址控制等功能。在 FTP 服务器安全管理中，主要设置禁止匿名用户访问、NTFS 访问权限和磁盘配额等功能。除此之外，服务器配置文件和站点主目录的备份也是非常重要的。

习　　题

1. IIS 7.0 与 IIS 6.0 相比有了哪些安全改进？
2. 如何备份基于 IIS 7.0 的 Web 服务器配置信息？
3. 用户可以通过那些方法确保 FTP 服务器的安全？

实验：保护 Web 服务器安全

实验目的

掌握保护 IIS 7.0 安全的主要措施。

实验内容

通过各种措施，确保基于 IIS 7.0 的 Web 服务器和站点的安全。

实验步骤

1. 为 Web 站点主目录设置 NTFS 访问权限。
2. 为指定虚拟目录设置内容过期期限。
3. 设置基本身份验证方式。
4. 禁止指定 IP 地址的用户访问网站。

第15章

Windows 防火墙

Windows Server 2008 的防火墙是一款基于主机的状态防火墙，已经被预先安装，与 Windows Server 2003 相比不仅安全性高，而且易于管理和配置。具有高级安全性的 Windows 防火墙结合了主机防火墙和 IPSec，在计算机上运行时，对可能穿越边界网络或源于组织内部的网络攻击提供本地保护。不仅如此，还提供计算机到计算机的安全连接，轻松实现对通信要求身份验证和数据保护。

本章导读

- Windows 防火墙的基本配置
- 使用命令行配置 Windows 防火墙
- 使用组策略配置 Windows 防火墙
- Windows 防火墙事件审核配置



15.1　Windows 防火墙

默认状态下，Windows 防火墙已经处于开启状态，能够提供基本的安全防护功能，保护内部网络免受恶意攻击者的入侵。当然，除了使用默认配置外，用户还可以根据需要开启或关闭防火墙。在 Windows Server 2008 中，Windows 防火墙的基本配置变化不大，拥有系统管理员权限的用户帐户，就可以在控制面板中打开并配置 Windows 防火墙。

15.1.1　Windows 防火墙概述

Windows Server 2008 系统的帐户控制功能默认是启用的，普通帐户必须得到管理员帐户的授权后，才可以配置 Windows 防火墙。依次选择“开始”→“控制面板”命令，打开“控制面板”窗口。单击“经典视图”超级链接，切换到经典模式，双击“Windows 防火墙”图标，打开“Windows 防火墙”窗口。单击“更改设置”超级链接，即可打开“Windows 防火墙设置”对话框。

1. “常规”选项卡

在如图 15.1 所示“常规”选项卡中，可以为所有连接启用或关闭 Windows 防火墙，而且“阻止所有传入连接”也是一个非常好用的选项，特别是当前连接到的网络存在严重的安全隐患时，该选项能够临时让系统禁止“例外”选项卡中设置的任何程序或服务访问网络，一旦本地服务器系统处于一个比较安全的工作环境时，再取消“阻止所有传入连接”选项的选中状态，恢复之前的正常操作。

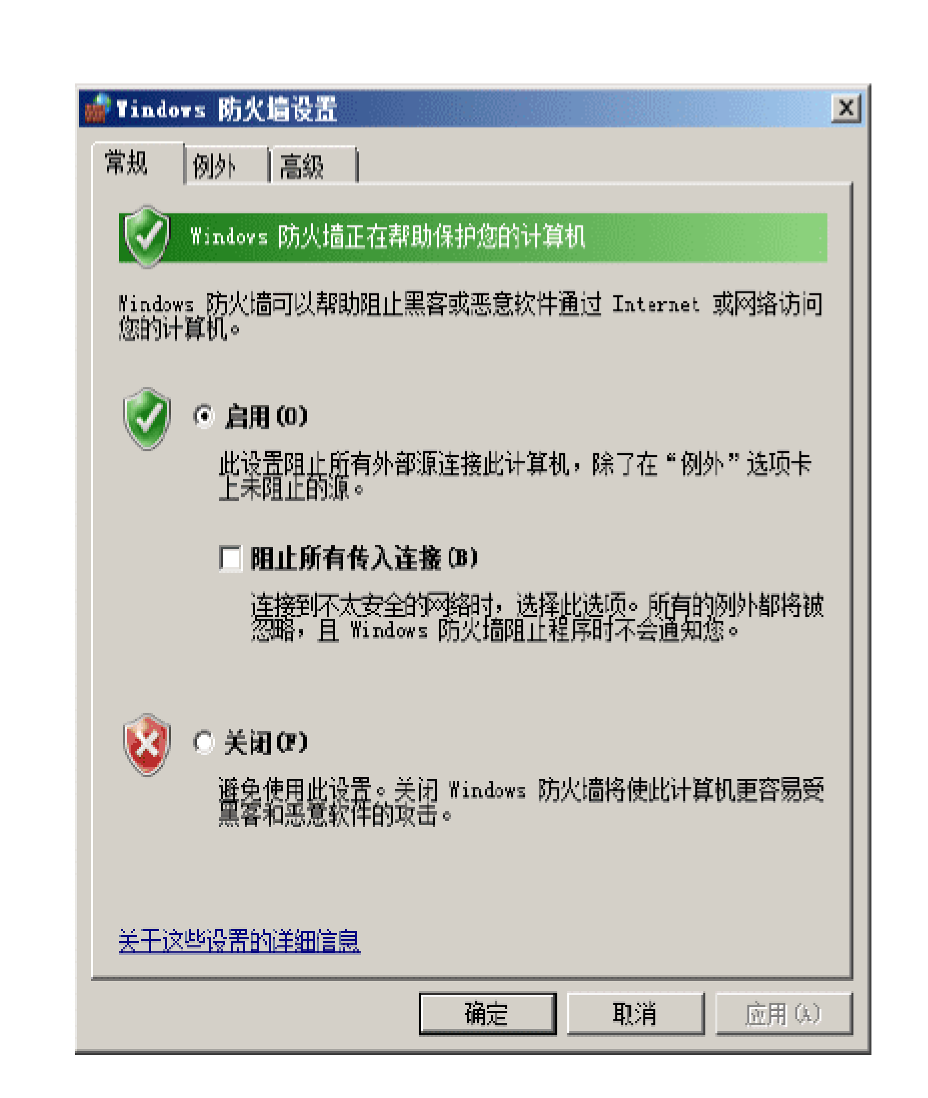


图 15.1　“常规”选项卡

启用了服务器系统的防火墙功能后，在默认状态下，该防火墙程序会同时拦截所有程序去访问外部网络，除了在“例外”选项卡中设置的选项外。

Windows 防火墙有 3 种设置：

- 启用。Windows 防火墙在默认情况下是处于打开状态的，通常情况下，建议保留此设置。此时，Windows 防火墙会阻止所有到计算机的未经请求的连接，但不包括在“例外”选项卡中选中的程序或服务所发出的请求；
- 启用时阻止所有传入连接。如果选中“阻止所有传入连接”复选框，则 Windows 防火墙会阻止所有到计算机的未经请求的连接，“例外”选项卡中的程序和服务也将不能连接网络。使用该设置可以为计算机提供最大程度的保护。需要注意的是，此时某些程序可能会无法正常工作；

- 关闭。如果关闭 Windows 防火墙，则计算机很容易受到非法入侵者或 Internet 病毒的侵害。此设置只适用于高级用户，或计算机有第三方防火墙的保护下使用。

2. “例外”选项卡

在如图 15.2 所示“例外”选项卡中设置能够直接访问网络的程序或服务，可以直接通过单击“添加程序”、“添加端口”按钮来自行添加需要访问外部网络的程序或服务，解除系统防火墙程序对网络访问的阻止。

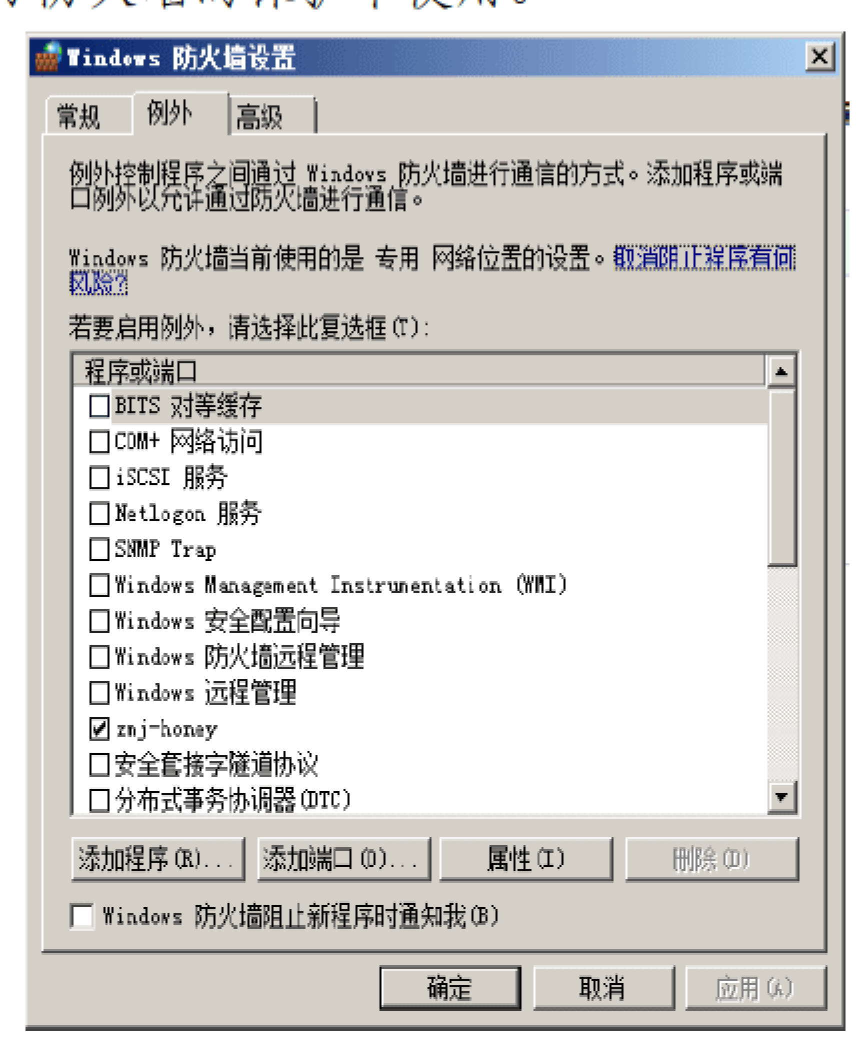


图 15.2 “例外”选项卡

3. “高级”选项卡

在如图 15.3 所示“高级”选项卡中，可以根据本地服务器系统中多条网络连接的情况，选择需要受防火墙保护的目标网络连接。如果发现防火墙中有许多参数没有配置正确，或防火墙出现故障，用户可以直接单击“还原为默认值”按钮，快速取消所有的参数修改操作，将系统防火墙的参数设置恢复到系统起初安装时的状态。

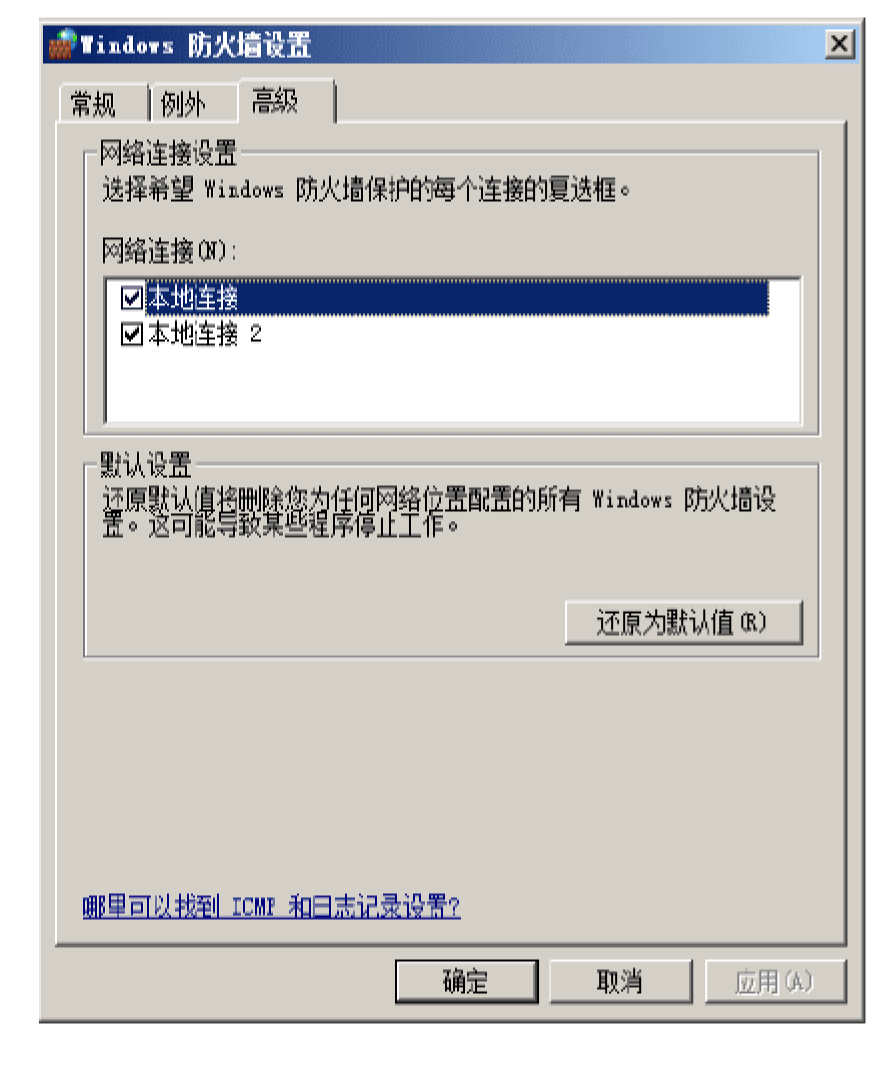


图 15.3 “高级”选项卡

注意



还原为默认值后，用户自定义的所有“例外”项目都将被删除，所有设置和选项都还原到原始状态。

使用“还原为默认值”按钮，可能会使 Internet 连接共享（ICS）和网桥出现故障，显示如图 15.4 所示“还原为默认值确认”对话框。

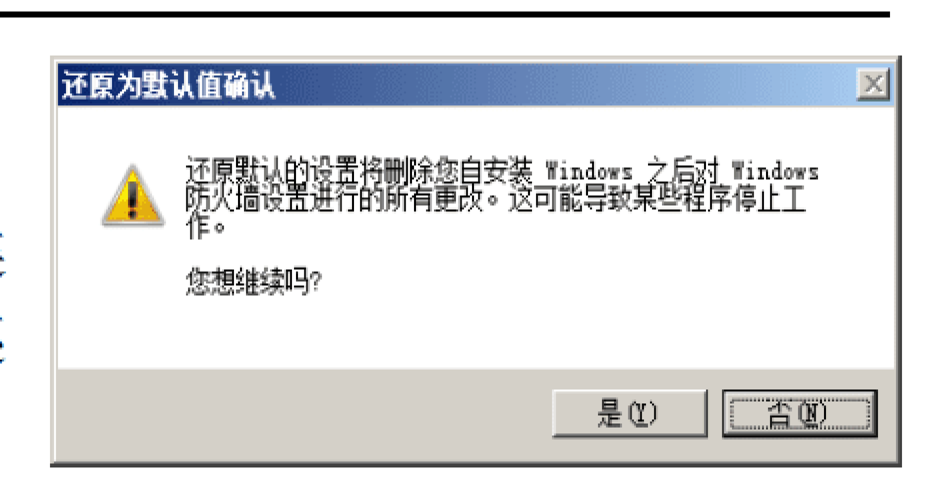


图 15.4 “还原为默认值确认”对话框

15.1.2　允许/限制端口访问

端口可以认为是计算机与外界通信交流的出口。开启的端口在提供网络应用的同时，很可能成为恶意用户入侵的通道。打开端口就像是在防火墙上打一个漏洞，如果在防火墙上有太多这样的漏洞，防护作用将会受到严重的影响。通常情况下，开放端口时应遵循以下原则：

- 只有当真正需要的打开某个端口时，才能将该端口打开；
- 决不为未识别的程序打开端口；
- 一旦不再需要端口，立即将其关闭。

1. 设置端口访问策略

01 打开“Windows 防火墙设置”对话框，切换到“例外”选项卡。单击“添加端口”按钮，打开如图 15.5 所示“添加端口”对话框。在“名称”文本框中，输入名称，例如 MSN；在“端口号”文本框中，输入要添加的端口号，例如 1863；选中“TCP”单选按钮。

注意



如果无法确定要使用哪个端口号，或者无法确定选择 TCP 还是 UDP 时，可通过查看要为其添加端口的程序或服务的文档或网站即可。

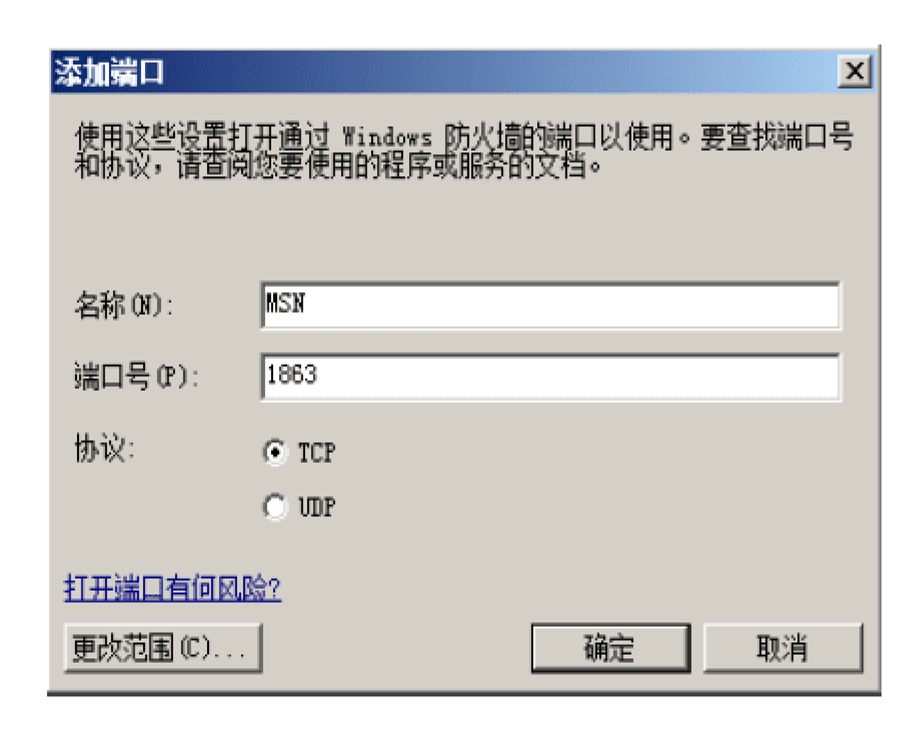


图 15.5　“添加端口”对话框

02 单击“更改范围”按钮，显示如图 15.6 所示“更改范围”对话框，选中“任何计算机（包括 Internet 上的计算机）”单选按钮。另外两项的意义分别是：

- “仅我的网络（子网）”：只允许从本地子网进行连接；
- “自定义列表”：定义自定义列表，输入以逗号隔开的 IP 地址，子网可同时包括 IP 地址、子网列表。

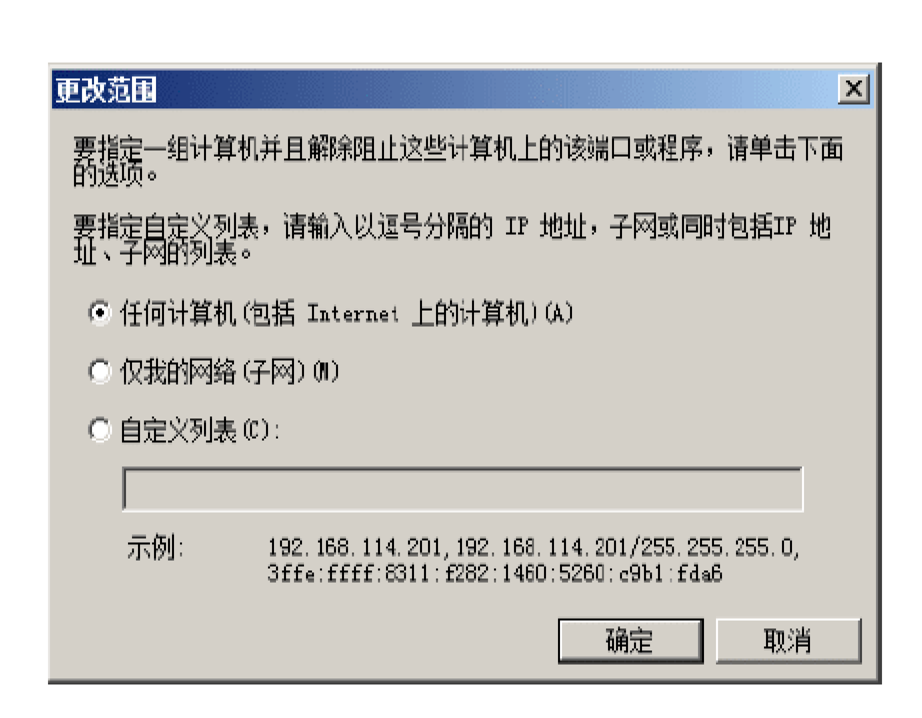


图 15.6　“更改范围”对话框

03 单击“确定”按钮，完成端口策略的创建。显示如图 15.7 所示。

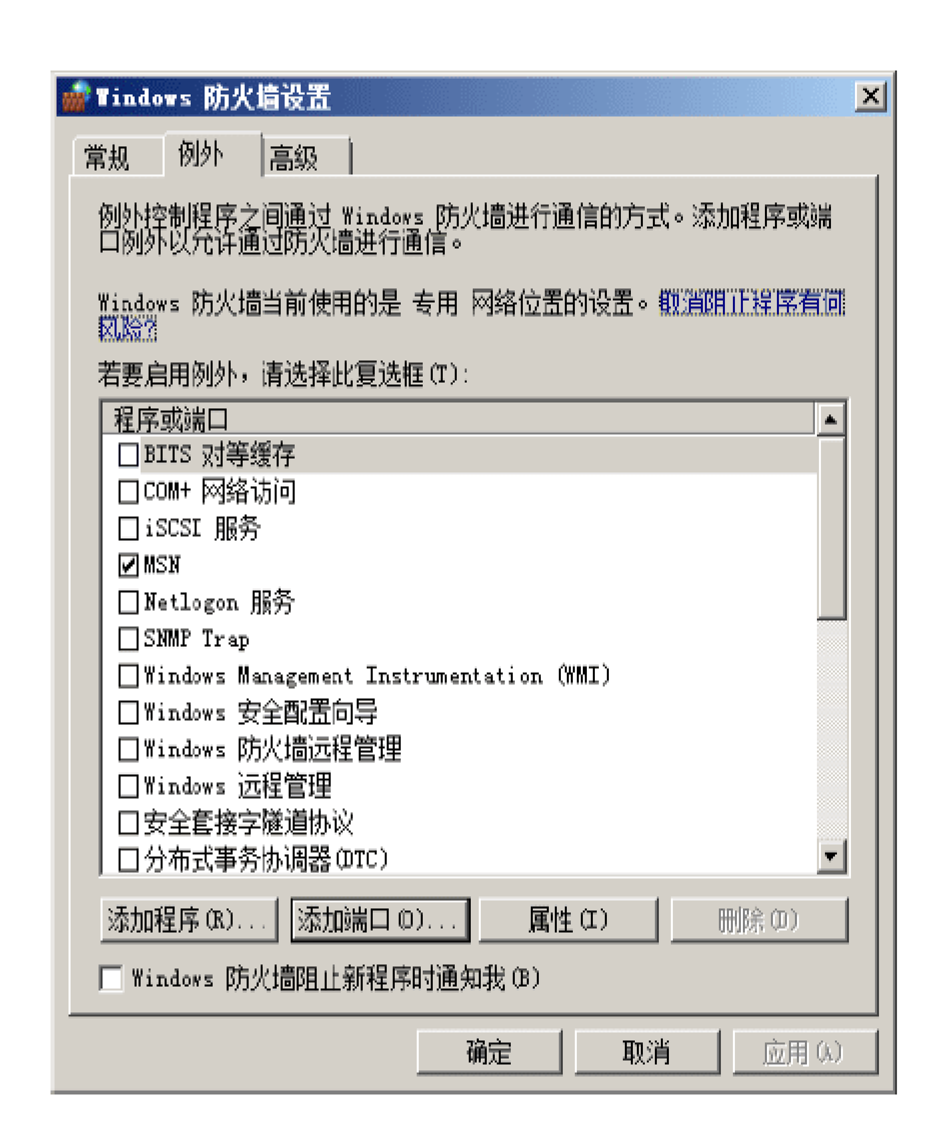


图 15.7 新创建的端口策略

提示 向例外列表添加端口会降低计算机的安全性，这是因为只要计算机在运行，该例外端口都是打开的。因此建议用户只有在无法添加例外程序时，才应该将端口添加到例外列表。

2. 删除端口例外

本地用户或者被委派了适当权限的用户帐户，可以删除用户自定义的“例外”项目，只需在“程序和端口”列表中，选中欲删除的项目，单击“删除”按钮即可。例如删除刚刚创建的 MSN 项目，显示如图 15.8 所示“删除端口”对话框，继续单击“是”按钮，即可从列表中删除。

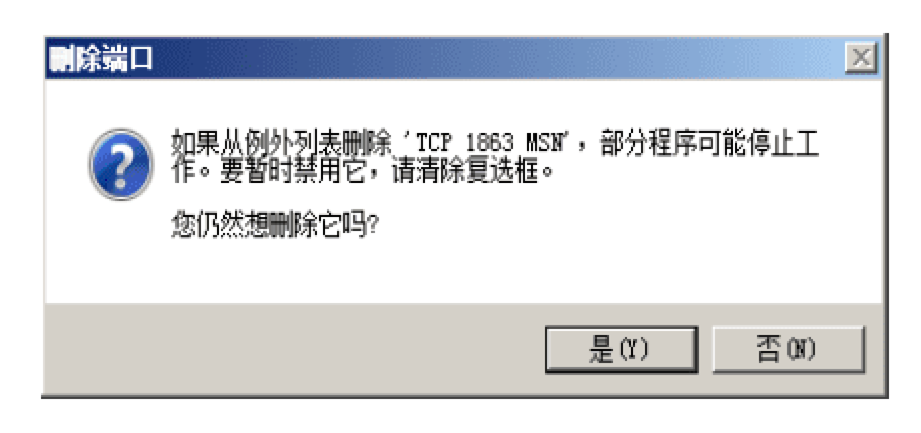


图 15.8 “删除端口”对话框

15.1.3 允许/限制程序访问

为了提高系统的安全性，默认情况下 Windows 防火墙阻止所有与计算机程序建立的未经请求的连接，导致用户许多正常网络应用无法实现。因此，需要对这些程序进行设置，在防火墙中为这些程序创建例外，应用程序即可通过防火墙访问网络。

1. 允许例外的风险

每次允许例外程序通过 Windows 防火墙通信时，计算机都会面临被攻击的危险。如果在计算机上存在很多例外和开放的端口时，计算机很容易成为入侵者的牺牲品。为了减少由于例外所引起的风险，一般添加到例外中的程序应进行如下操作：

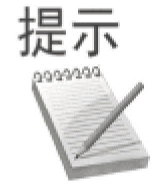
- 只有在真正需要时才允许例外；
- 对于不认识的程序从不允许例外；
- 不再需要例外时删除例外。

2. 向“例外”列表中添加程序



要允许与计算机程序建立未经请求的连接，只需将应用程序添加到 Windows 防火墙的“例外”列表中即可。

01 打开“Windows 防火墙设置”对话框，切换到“例外”选项卡。单击“添加程序”按钮，显示如图 15.9 所示“添加程序”对话框。在“程序”列表中，选择要允许访问网络的应用程序即可。



提示 单击“更改范围”按钮，同样可以为添加的“例外”程序设置适当的作用范围，与“允许/限制端口访问”中的操作完全相同，此处不复赘述。

02 单击“确定”按钮，将其添加到“例外”选项卡的“程序和端口”列表中。

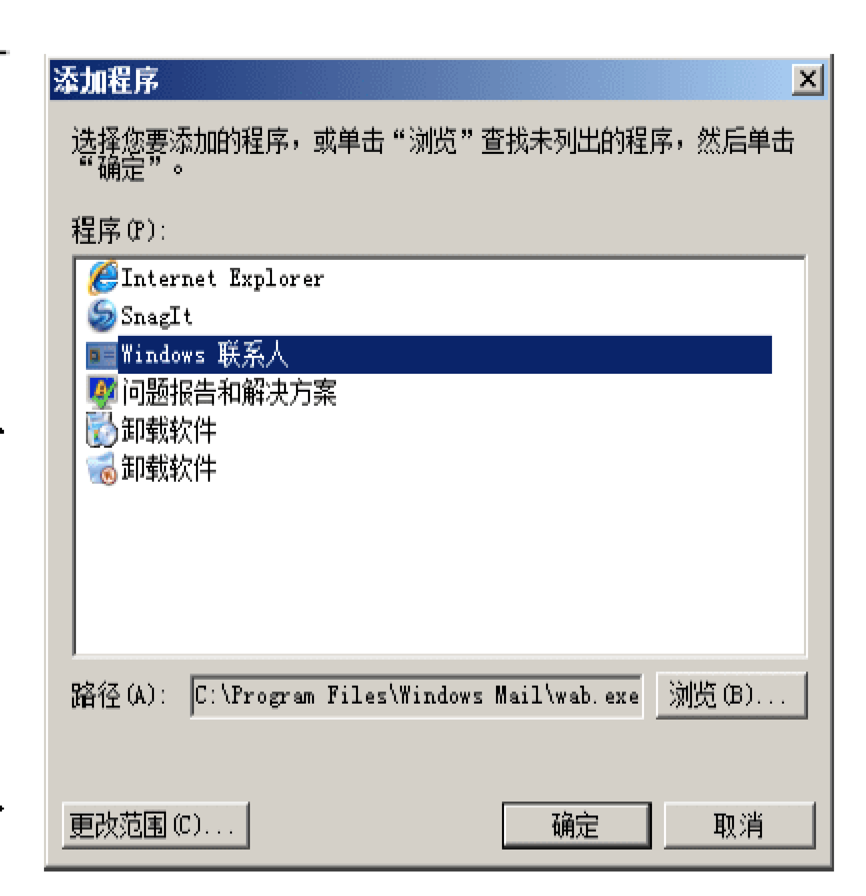


图 15.9 “添加程序”对话框

3. 编辑/删除程序例外

在“例外”选项卡的“程序和端口”列表中，选中希望编辑或删除的应用程序项目，单击“属性”按钮，即可查看其相关信息。例如，选择“Internet Explorer”选项，单击“属性”按钮，显示如图 15.10 所示“编辑程序”对话框。单击“更改范围”按钮，可以重新编辑当前例外程序的作用范围。

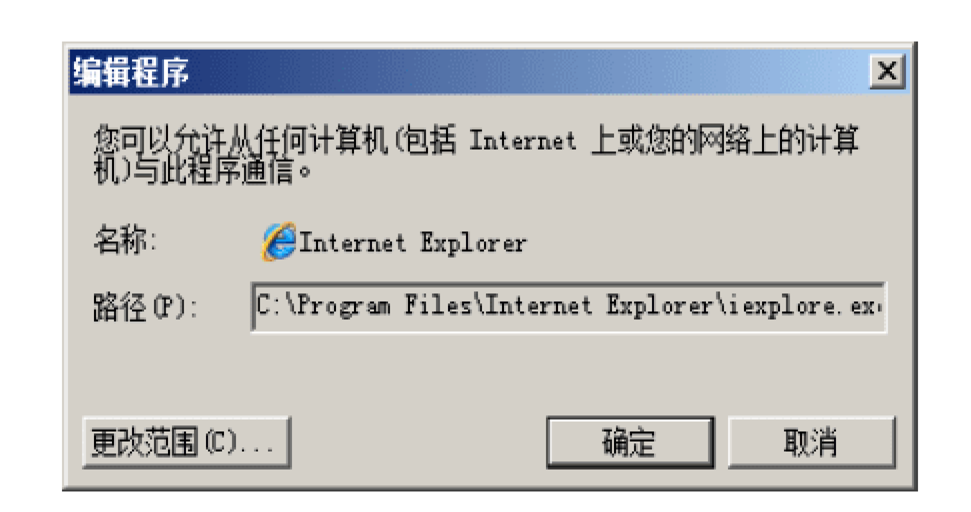
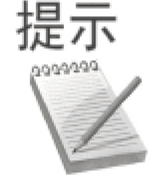


图 15.10 “编辑程序”对话框



提示 如果选中应用程序选项后，单击“删除”按钮，则直接从列表中删除所选程序。与端口例外相同，用户只能删除自定义的程序项目。

15.2 高级安全 Windows 防火墙基本配置

高级安全 Windows 防火墙是 Windows Server 2008 的新增功能之一，与标准 Windows 防火墙相比，安全防护能力更强，具有以下特点：

- 高级安全 Windows 防火墙是双向防火墙，其不仅可以监视、设置甚至屏蔽所有的入站连接请求（默认设置为禁止），也可以对所有的出站连接请求进行更细致的设置（默认设置为允许）；
- 高级安全 Windows 防火墙是一种基于规则状态防火墙，支持 IPv4 与 IPv6，远比应用层

级的边界防火墙更为安全；

- 高级安全 Windows 防火墙结合了主机防火墙和 IPSec，而在 Windows XP/2003 系统中，Windows 防火墙与 IPSec 是分离的。

15.2.1 高级安全 Windows 防火墙概述

早期的 Windows 系统并未提供防火墙功能，从 Windows XP SP1 系统才开始提供，直到出现 Windows Vista/2008 之前，防护功能都比较单一，只可以阻止未经请求的连接。一些比较复杂的网络攻击，往往需要通过监视通信或者伪装通信来实现，因此需要更加可靠的安全防护。Windows Server 2008 系统中的高级安全 Windows 防火墙，集成了 IPSec 管理，IPSec 通过双方的认证和加密来降低这种攻击的可能性。

1. 使用 Windows 防火墙筛选通信

管理员可以借助 Windows 防火墙，控制哪些服务可以连接网络，哪些网络可以连接特定的服务。默认情况下，Windows 防火墙允许所有发出通信通过，但是管理员也可以限制应用程序发送通信。管理员可以创建如下形式的防火墙规则：

- 在 DNS 服务器上，只允许内部网络的请求消息；
- 在 E-mail 服务器上，允许所有计算机通过 TCP 端口 25 连接 SMTP 服务器，同时只允许内网计算机使用 TCP 端口 110 连接 POP 服务器；
- 除了 Windows 更新之外阻止所有的应用程序和服务向外连接网络；
- 允许内网计算机对服务器使用“ping”命令，但是阻止响应来自 Internet 的“ping”请求。

2. 使用 IPSec 保护通信

IPSec 是网络层提供认证和加密安全标准，是 TCP/IP 协议的一部分。IPSec 可以有效防护探测攻击。例如网络中的共享文件没有提供任何加密措施，攻击者通过访问物理网络就可以读取到传输中的文件内容。通过 IPSec 可以对网络通信进行加密，从而使攻击者基本不可能看到传输的文件内容。

（1）IPSec 的身份验证功能

除了加密功能外，IPSec 还提供认证功能。通过认证功能，服务器上的 IPSec 在客户端连接之前就可以确定该客户端是否是域成员或者拥有一个有效地计算机证书。同样，客户端计算机也可以确定正确的服务器。IPSec 认证可以有效阻止常见的“中间人”攻击，如图 15.11 所示。

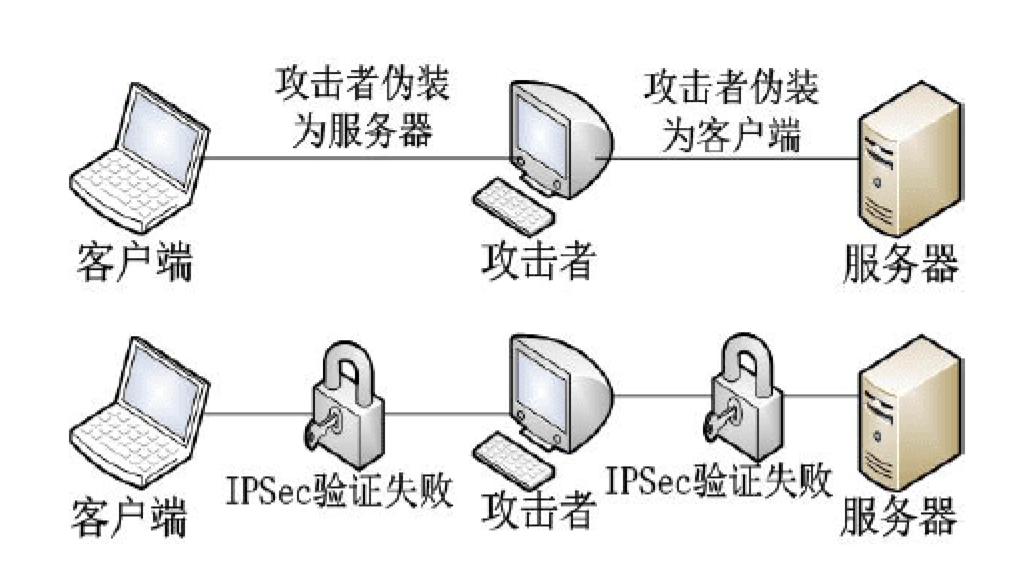


图 15.11 IPSec 阻止“中间人”攻击



总之，IPSec 可以阻止如下行为：

- Man-in-the-middle 攻击；
- 探测攻击；
- 重放攻击；
- 未认证的网络应用程序的访问；
- 只使用客户端 IP 地址进行认证的网络应用程序的访问。

因为 IPSec 在网络层操作，所以对于大多数应用程序来说它是透明的；但是对于有些网络设备来说 IPSec 是不兼容的。任何一个防火墙或检查通信的其他设备都是不允许 IPSec 加密传输的，所以用户需要经常配置这些设备来允许 IPSec 通信。

（2）IPSec 的工作模式

IPSec 有两种模式：传输模式和通道模式。传输模式用来保护主机到主机的通信。在传输模式中，IPSec 通信在第 4 层传输层（OSI 参考模型），所以 IPSec 可以加密 UDP/TCP 协议包头和原始数据，但是 IP 包头确不能被保护。通道模式用来保护主机到网络和网络到网络的通信，如 VPN。IPSec 将数据压缩到包头和包尾。按照 IPSec 协议，发送出去的数据包的原始内容将会被加密。IPSec 使用压缩安全负载（ESP）协议来提供认证和加密的。如图 15.12 所示 IPSec 的 IPv4 传输模式的数据包结构。

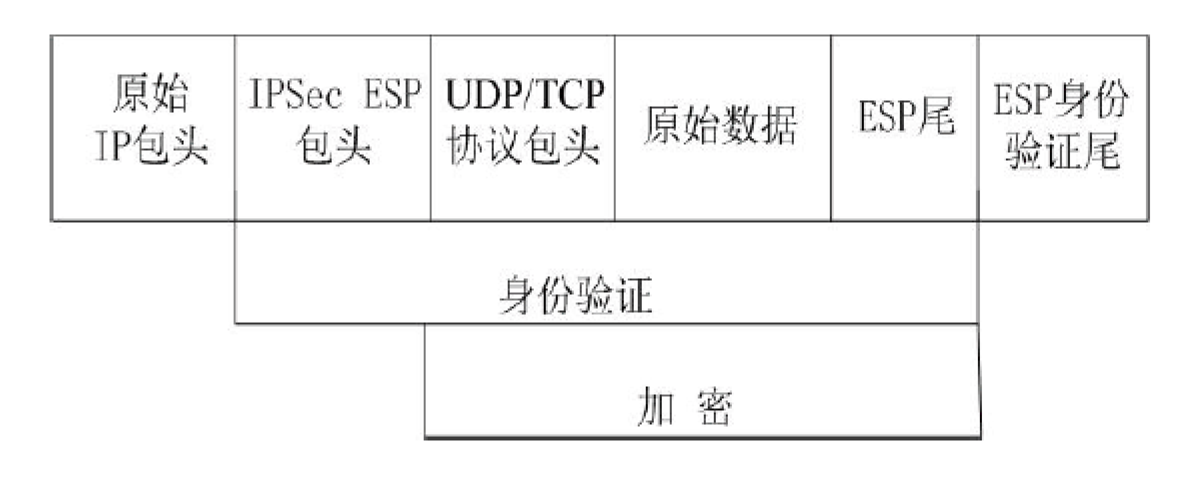


图 15.12　IPSec 数据包结构

注意



IPSec 也是 IPv6 的一部分。

应用 IPSec 加密之前需要注意的是，并不是所有的计算机都支持 IPSec。IPSec 支持多种认证和加密标准，两台支持 IPSec 的主机可能支持的是不同类型的标准。因此，在建立 IPSec 连接之前，必须确定这些主机是否都支持 IPSec 和一系列可接受的认证和加密标准。

IKE（Internet 密钥交换协议）是 Internet 安全关联和密钥管理协议（ISAKMP）和 Oakley 密钥交换协议的组合，主要用于管理在 IPSec 连接中使用的加密密钥算法。Windows Vista 和 Windows Server 2008 系统支持的 IKE 协商模式如下。

- 主模式：IKE 协商认证和加密协议，然后认证计算机；
- 用户模式：如果用户认证是为 IPSec 配置的，那么 IKE 认证用户；
- 快速模式：IKE 保护个人通信传输，并且经常改变安全密钥，但是在该模式下无法进行认证。

（3）认证头和 ESP

IPSec 使用如下两种协议。

- 认证头（AH）：AH 对整个 IP 数据包进行认证，但不进行数据加密，适用于某些要求严格防止 IP 欺骗的场合，所以在 NAT 模式下无法使用；
- ESP：同时提供对数据加密和认证，ESP 认证不对外部 IP 头进行认证，所以可以在 NAT 模式下使用。

默认情况下，Windows 系统将自动尝试使用 ESP 协议，当两台主机都不支持 ESP 协议时，才尝试使用 AH 协议。由于 ESP 协议广泛的支持性，AH 协议很少用到。

3. 相关概念

高级安全 Windows 防火墙使用两组规则，配置如何响应传入和传出流量，确定允许或阻止流量类型。连接安全规则确定如何保护计算机与计算机间的通讯，通过使用防火墙配置文件，可以应用这些规则以及其他设置，监视防火墙活动和规则。

（1）防火墙规则

配置防火墙规则以确定阻止还是允许流量通过。传入数据包到达计算机时，高级安全 Windows 防火墙会检查该数据包，确定其是否符合防火墙规则中指定的标准。如果数据包与规则中的标准匹配，高级安全 Windows 防火墙执行规则中指定的操作，即阻止连接或允许连接。如果数据包与规则中的标准不匹配，高级安全 Windows 防火墙将丢弃该数据包，并在防火墙日志文件中创建条目。

（2）连接安全规则

连接安全规则可以用来配置本地计算机与计算机之间特定的连接的 IPSec 设置。高级安全 Windows 防火墙首先使用该规则评估网络通信，然后根据该规则中所建立的标准，阻止或允许消息。默认状态下，高级安全 Windows 防火墙将阻止通信。如果所配置的设置要求连接安全（双向），而两台计算机无法互相进行身份验证，同样会阻止连接。

（3）防火墙配置文件

防火墙配置文件是一种分组设置的方法，如防火墙规则和连接安全规则，根据计算机连接到的位置将其应用于该计算机。高级安全 Windows 防火墙中有 3 个配置文件，分别是域、专用网络（例如家庭网络）和公用网络，用户每次只能从中选择一个使用。

（4）监视

监视节点显示有关当前所连接的计算机（本地计算机或远程计算机）的信息。如果使用管理单元来管理组策略对象而不是本地计算机，不会出现该节点。



15.2.2　配置防火墙规则

以管理员帐户登录 Windows Server 2008 系统后，选择“开始”→“管理工具”→“高级安全 Windows 防火墙”命令，打开如图 15.13 所示“高级安全 Windows 防火墙”窗口，包括入站规则、出站规则和连接安全规则 3 种。如果安装 Active Directory 服务，还会增加 13 条相应的安全规则。

- 入站规则。入站规则明确允许或者明确阻止与规则条件匹配的通信。例如，可以将规则配置为明确允许受 IPSec 保护的远程桌面通信通过防火墙，但阻止不受 IPSec 保护的远程桌面通信。首次安装 Windows 时，将阻止入站通信，若要允许通信，必须创建一个入站规则。在没有适用的入站规则的情况下，也可以对具有高级安全性的 Windows 防火墙所执行的操作进行配置；
- 出站规则。出站规则明确允许或者明确拒绝来自与规则条件匹配的计算机的通信。例如，可以将规则配置为明确阻止出站通信通过防火墙到达某一台计算机，但允许同样的通信到达其他计算机。默认情况下允许出站通信，因此必须创建出站规则来阻止通信。



图 15.13　“高级安全 Windows 防火墙”窗口

1. 禁用或启用规则

管理员可以通过两种方式启用或禁用防火墙规则：Windows 防火墙控制台和 netsh 命令。

第一种方式:

在高级安全 Windows 防火墙控制台中，选择“入站规则”或“出站规则”选项，在右侧窗口中，选择并右击相应的规则，选择快捷菜单的“禁用规则”或者“启用规则”选项，即可更改其运行状态。

第二种方式：

使用“netsh”命令启用或禁用单一规则以及规则组，用法如下：

- 启用/禁用单个规则：netsh advfirewall firewall set rule name="*Rule*" new enable=yes | no；
- 启用/禁用规则组：netsh advfirewall firewall set rule name=" *RuleGroup*" new enable=yes | no

例如，使用如下命令可以启用“BITS 对等缓存（RPC）”规则（默认情况是禁用的）：

```
netsh advfirewall firewall set rule name="BITS Peercaching （RPC）" new enable=yes;
```

使用如下命令可启用“BITS 对等缓存”规则组的（默认情况是禁用的）：

```
netsh advfirewall firewall set rule group="BITS Peercaching" new enable=yes。
```

2. 创建防火墙规则

创建防火墙规则，其目的是允许此计算机向程序、系统服务、计算机或用户发送通信，或者从程序、系统服务、计算机或用户接收通信。通过创建防火墙规则，可为匹配该规则标准的所有连接执行以下三个操作之一：允许连接、只允许通过 Internet 协议安全（IPSec）保护的连接或者明确阻止连接。可以为入站通信或出站通信创建规则，可以指定要应用规则的网络适配器类型：局域网、无线、远程访问，也可以将规则配置为在使用特定配置文件时应用，或者在使用任何配置文件时应用。

01 在高级安全 Windows 防火墙控制台中，右击“入站规则”选项，选择快捷菜单中的“新规则”选项，在“规则类型”对话框，选中“端口”单选按钮。单击“下一步”按钮，显示“协议和端口”对话框，选中“TCP”和“特定本地端口”单选按钮，输入服务使用的端口号，如果在配置服务器时指定了非默认端口，在这里也应指定相应端口，例如 80，如图 15.14 所示。

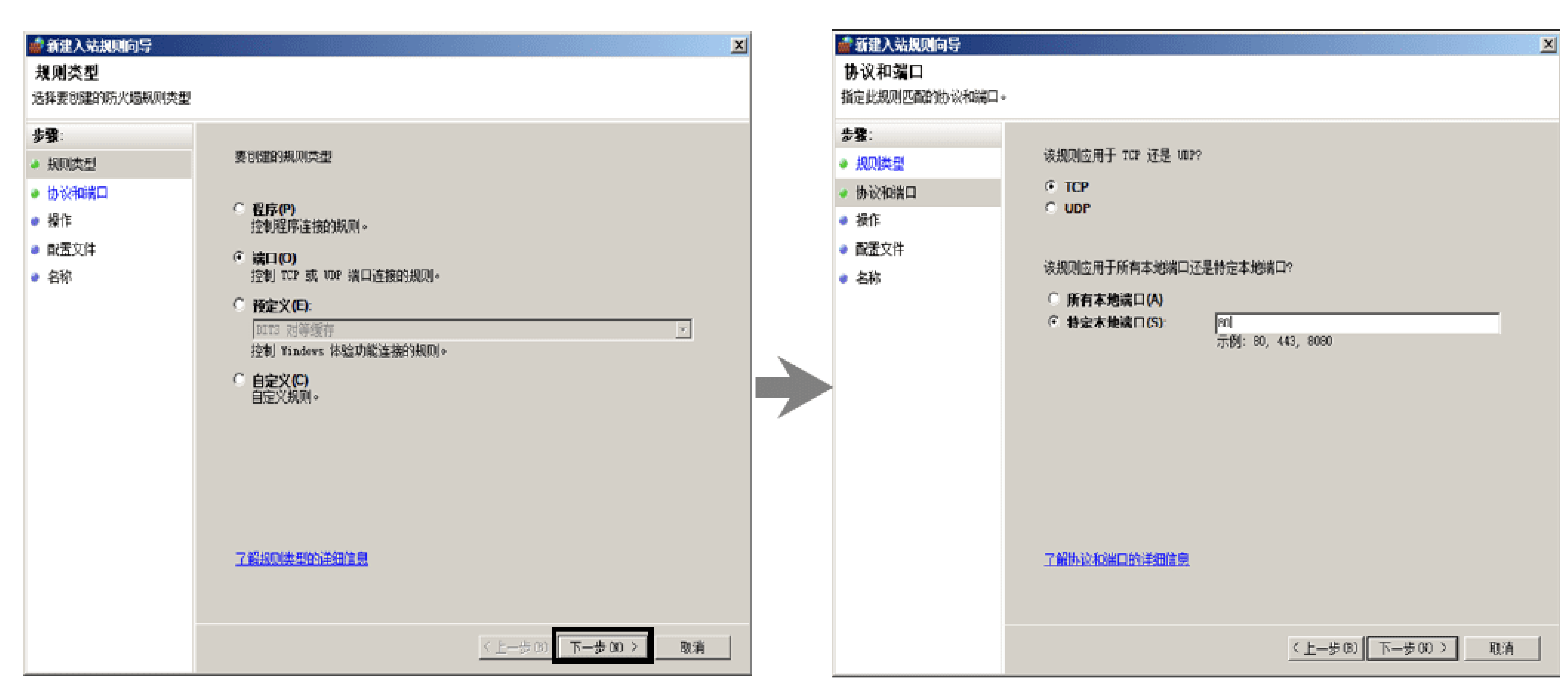


图 15.14　设置规则类型、协议和端口

02 依次单击“下一步”按钮，设置操作类型和配置文件，如图 15.15 所示。在“操作”对话框中，选中“允许连接”单选按钮。在“配置文件”对话框中，设置该规则的应用范围，选中“公用”复选框。其他操作类型的含义如下：



- 只允许安全连接：高级防火墙只允许特定的安全用户访问服务器，即使用 IPSec 身份验证的用户；
- 阻止连接：将阻止所有用户到服务器的连接。





图 15.15　设置操作类型和配置文件

03 单击“下一步”按钮，显示如图 15.16 所示“名称”对话框。在“名称”文本框中输入该入站规则的显示名称，便于识别。在“描述”文本框中，可以输入相关的描述信息。

04 单击“完成”按钮，即可保存已创建的入站规则。FTP 服务器提供下载和上传服务时，需要使用不同的端口，因此还需要对用于发布上传服务的端口创建入站规则。

默认情况下，成功创建的入站规则将自动启用，并显示在“入站规则”窗口中，如图 15.17 所示。

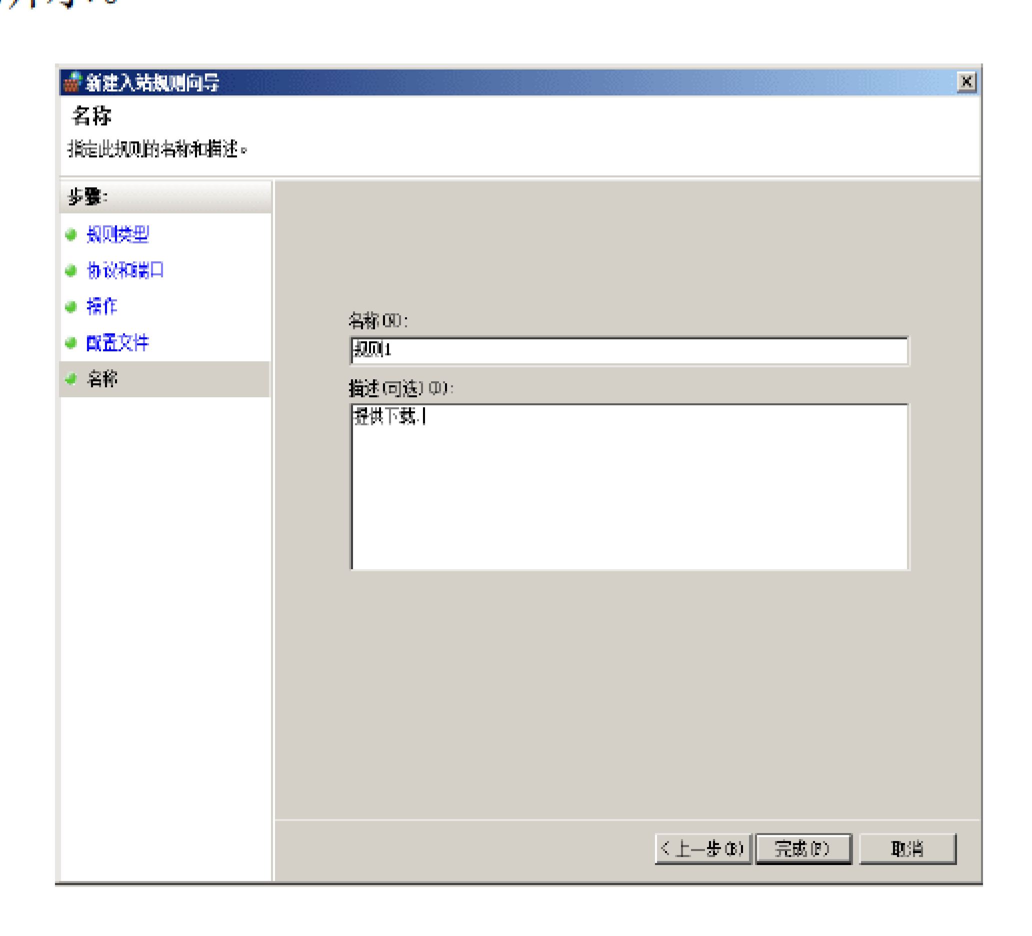


图 15.16　“名称”对话框

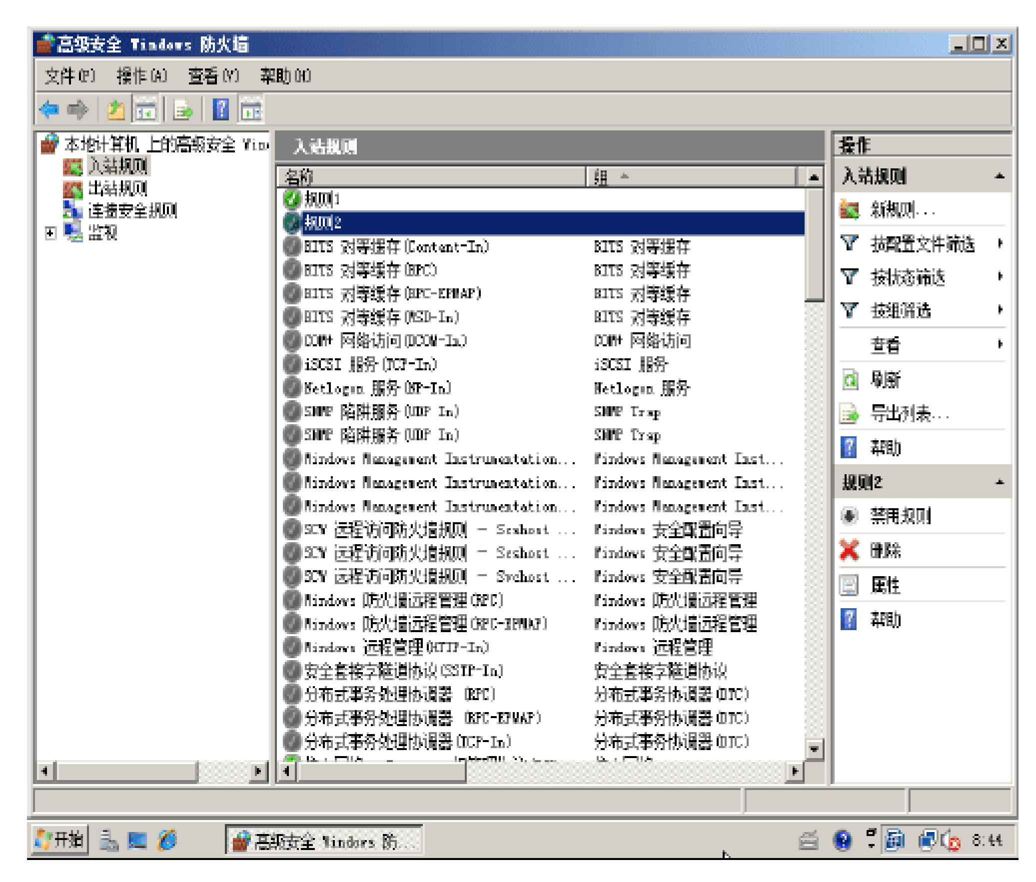


图 15.17　成功创建的入站规则

3. 编辑防火墙规则

在 Windows Server 2008 系统中，ICMP 协议的防火墙规则已被默认集成在高级安全 Windows 防火墙中的出站/入站规则中。用户可以通过修改配置，达到禁止响应 ping 或者禁止 ping 出的目的，以确保服务器安全。

01 在高级安全 Windows 防火墙控制台中，选择“入站规则”或“出站规则”选项，右击需要配置的规则（以“网络发现（LLMNR-UDP-In）”策略为例），在快捷菜单中选择“属性”命令，打开如图 15.18 所示“网络发现（LLMNR-UDP-In）属性”对话框。在“常规”选项卡中，选中“只允许安全连接”单选按钮即可启用 IPSec 保护。

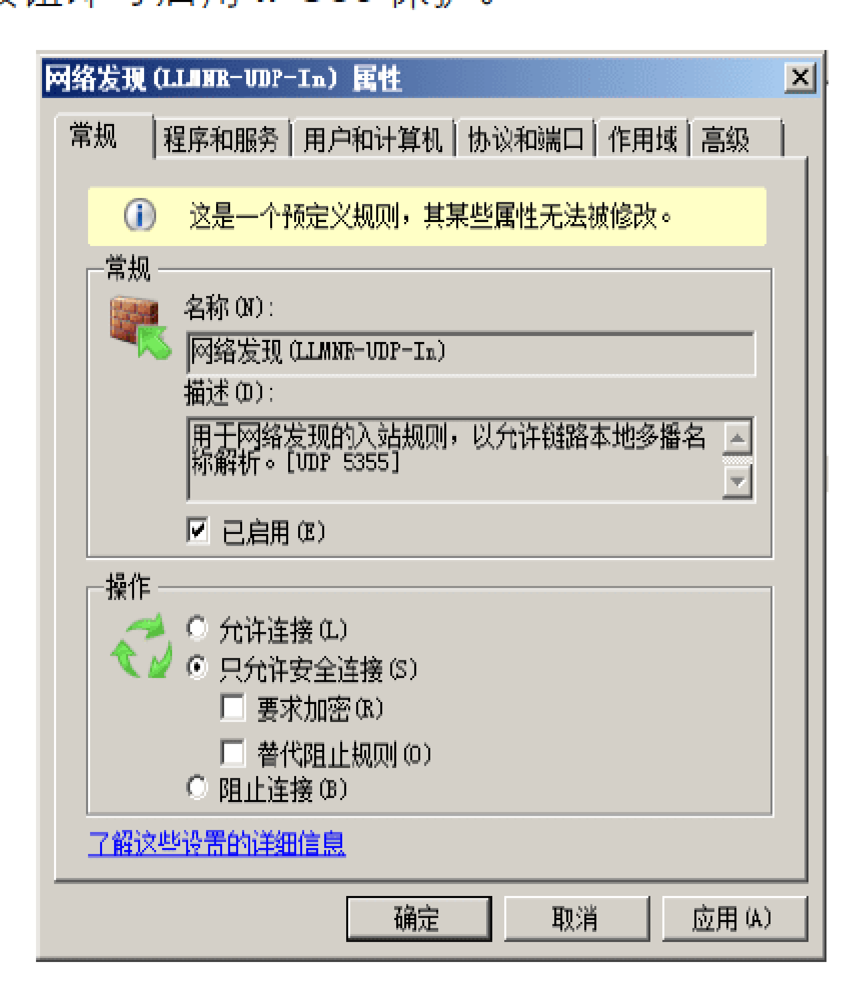


图 15.18 “网络发现（LLMNR-UDP-In）属性”对话框

02 选择“作用域”选项卡，在本地 IP 地址下选中“下列 IP 地址”单选按钮，单击“添加”按钮，显示“IP 地址”对话框，打开如图 15.19 所示“IP 地址”对话框和，添加指定的本地或远程 IP 地址即可。

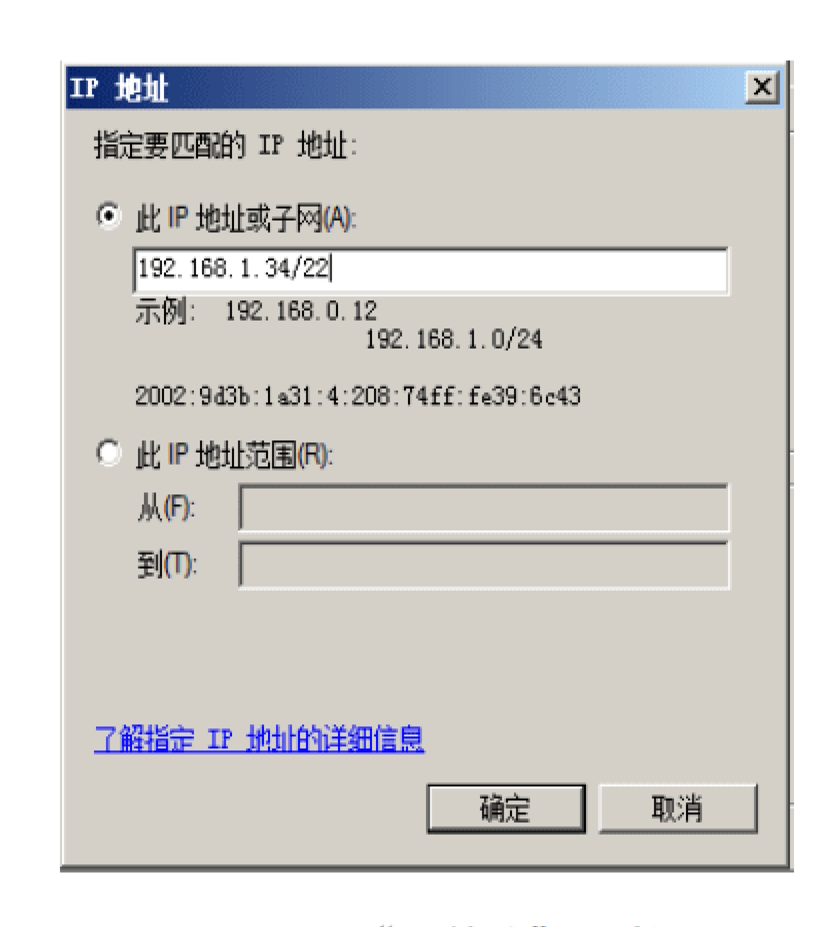


图 15.19 “IP 地址”对话框

03 单击“确定”按钮，返回到“网络-路由器请求属性”对话框。切换到“用户和计算机”选项卡，选中“只允许来自下列计算机的连接”或“只允许来自下列用户的连接”复选框，单击“添加”按钮，显示如图 15.20 所示“选择内置安全主体”对话框，添加计算机或用户。



图 15.20 “选择内置安全主体”对话框

04 单击“高级”按钮，切换到如图 15.21 所示“高级”选项卡，选中“下列配置文件”单选按钮，选择需要应用规则的配置文件：

- 域：当计算机连接到其域帐户所在的网络时应用；
- 专用：当计算机连接到不包括其域帐户的网络时应用，例如家庭网络。专用配置文件设置应该比域配置文件设置更为严格；
- 公用：当计算机通过公用网络连接到域时应用。由于计算机所连接到的公用网络通常无



法严格控制安全，因此公用配置文件设置应该最为严格。

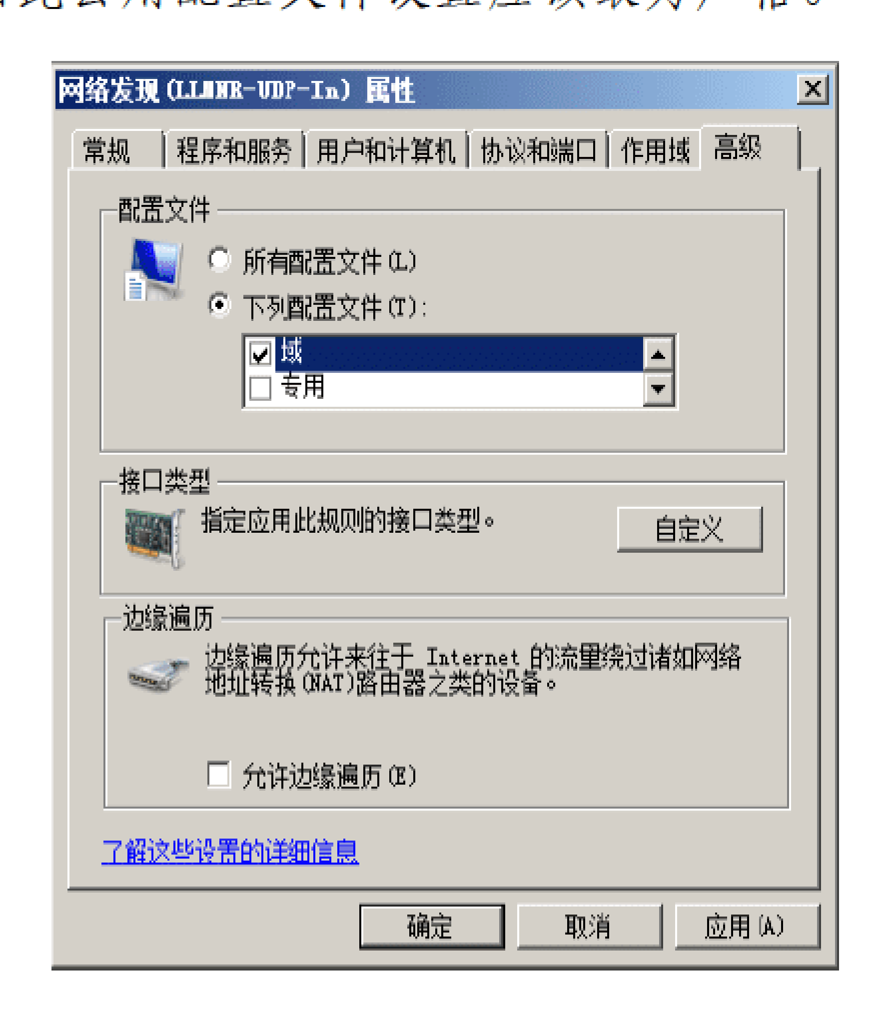


图 15.21　“高级”选项卡

05 修改规则完成后，单击“确定”按钮应用并保存配置。

15.2.3　配置 IPSec 连接安全规则

IPSec 即 Internet 协议安全，是网络安全技术的发展趋势，其主要功能是保护 IP 数据包内容和通过数据包筛选防御网络攻击。默认情况下，Windows Server 2008 拥有一个单一本地 IPSec 策略，该策略尝试对所有的通信使用 IPSec 认证和加密，当 IPSec 协商失败后将会退到不受保护的通信。用户必须为服务器或域隔离创建额外的规则来配置计算机。

1. IPSec 连接安全规则概述

IPSec 连接安全规则允许用户为满足指定标准的连接请求 IPSec，这些标准类似于 Windows 防火墙筛选器。例如，用户可以为如下情况设置 IPSec 安全规则：

- 拒绝来自指定 IP 地址的所有通信；
- 拒绝所有来自默认网关的 ICMP 通信；
- 拒绝所有来自内网的发往指定端口的通信；
- 限制除了特定服务器的所有出站连接。

每个计算机只能拥有一个 IPSec 策略。如果多个组策略应用于一台计算机，每个组策略都有不同的 IPSec 策略，只有最高级的 IPSec 策略会起作用。

（1）IPSec 规则类型

使用默认设置创建的 IPSec 规则是阻止用户通信的，即必需通过相应身份验证才可以。因此，应用之前必须确认要求认证连接的服务器和计算机，避免阻止合法用户的连接。如果环境允许，建议部署 IPSec 规则之前，在实验环境中进行测试。IPSec 连接安全规则的类型如下。

管理员可以创建如下几种类型的安全规则。

- 隔离：隔离规则可根据用户定义的身份验证标准对连接进行限制。例如可以使用此规则类型，隔离域中的计算机和域外的计算机；
- 身份验证免除：可以使用此规则类型，使特定的计算机或者指定范围内的 IP 地址（计算机），免于对自身进行身份验证，而不考虑其他连接安全规则；
- 服务器到服务器：使用此规则类型对两台特定计算机之间、两个计算机组之间、两个子网之间，或者特定计算机和计算机组或子网之间的通信，进行身份验证。可以使用此规则对数据库服务器和业务层计算机之间，或者基础结构计算机和其他服务器之间的流量，进行身份验证；
- 隧道：如果在不知 IPSec 的网络中，为支持 IPSec 的客户端和服务器创建 IPSec 连接安全规则，则必须使用隧道模式。这个类型的规则指定了使用隧道的主机和目的主机，以及本地和远端的网关。例如，VPN 或 IPSec L2TP 隧道等；
- 自定义：使用此规则类型创建需要特殊设置的规则。

注意 

若要创建身份验证免除规则，只需要指定计算机或者一组或一个范围内的 IP 地址（计算机）并给出规则的名称和说明（可选）即可。即使对计算机免除身份验证，防火墙仍可能阻止这些计算机，除非防火墙规则已明确允许其连接。

通常情况下，隔离规则用于应用所有网络连接的策略，服务器到服务器规则用于只应用在特定网络的策略，免除认证规则用于不支持 IPSec 的计算机。

（2）IPSec 认证方式

高级安全 Windows 防火墙可以提供如下几种身份验证方法。

- 默认值：选择此选项可使用“具有高级安全性的 Windows 防火墙属性”对话框的“IPSec 设置”选项卡上所配置的身份验证方法。默认值中的具体参数设置如表 15.1 所示；

表 15.1 Windows Server 2008 中默认 IPSec 设置

设置	值
认证方式	计算机（Kerbero V5）
密钥交换算法	Diffie-Hellman Group 2
数据完整性检查方法	SHA1
IPSec 认证协议	ESP
加密密钥周期	60 分钟或 100 000 KB
加密方法	AES-128（主）和 3-DES（备）

- 计算机和用户（Kerberos V5）：这种方法使用计算机和用户身份验证，只允许认证域用户的计算机的连接。首先进行计算机认证，然后使用 Kerberos V5 进行用户认证来添加一层额外保护；
- 计算机（Kerberos V5）：这种方法请求或要求计算机使用 Kerberos V5 身份验证协议进行身份验证，即只允许域成员的计算机的连接。为了 IPSec 使用 Kerberos 认证通过受信任区域，必须使用全资格域名（FQDN）来配置信任区域。另外，还需要配置 IPSec 客



户端策略，使其能够与任一域控制器进行通信，这样 IPSec 就可以从域控制器获取 Kerberos 通行证；

- 用户（Kerberos V5）：这种方法请求或要求用户使用 Kerberos V5 身份验证协议进行身份验证；
- 计算机证书：这种方法请求或要求使用有效的计算机证书进行身份验证。要使用这种方法，必须至少具有一个证书颁发机构（CA）。在使用证书认证的计算机之前，必须保证所有目标计算机都有正确的 CA 证书和相应的通行证书。此外，为了保证证书认证能预期工作，还需要在配置 IPSec 策略之前测试 PKI 基础设备；
- 高级：允许用户配置多种用户或计算机认证方式，并且指定相应的优先级。用户也可以为计算机认证使用预共享密钥，即为每个计算机配置一个密钥。因为预共享密钥在生产环境中很难改变，所以一般应用于试验环境，当任何一个计算机受到安全威胁时，就需要改变密钥。

注意  Kerberos V5 身份验证方法仅适用于 Windows 域环境，即只有计算机或用户帐户是域成员时，才可以使用该验证协议。

用户可以根据需要混合使用认证方式。例如配置公网 Web 服务器，对于内网用户可以使用 Kerberos 认证，对于外网用户可以使用公用密钥证书进行认证。在配置完 IPSec 之后，需要比较远程主机的 IP 地址和 IPSec 策略，然后决定使用哪种认证方式。

在使用 IPSec 之后，客户端就可以创建一条通向服务器的网络连接了，但是应用程序可能也需要认证。例如某个认证用户连接到一个需要认证的文件服务器上，当客户端尝试连接共享文件夹时，可能仍然需要认证。如图 15.22 所示是 IPSec 规则网络通信中的位置和作用示意图。

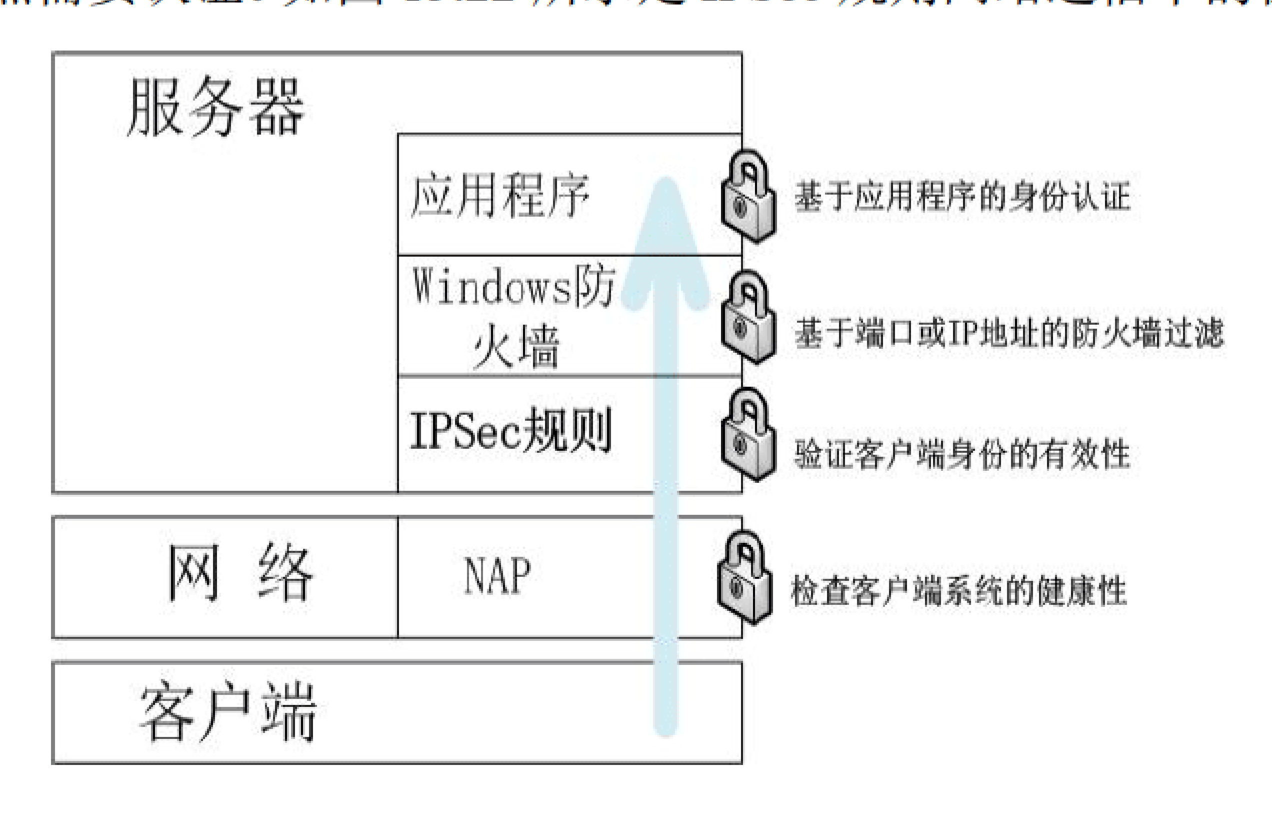


图 15.22　IPSec 是多层网络安全的一部分

（3）服务器和域隔离

“隔离”最初只是一种网络结构技术，即将计算机置于单独的物理网络中，使外网无法访问，从而阻止了未经认证的用户访问网络中的计算机。IPSec 认证能够提供高可靠性的逻辑隔离，该方式允许客户端连接各种网络。服务器和域隔离只允许认证用户建立网络连接。认证发生在网络层，从而有效地保护了网络通信。另外，IPSec 还会加密受保护的通信，防止攻击者通过物理网络截获数据。

- 域隔离：只有域成员才能建立网络连接；
- 服务器隔离：指定服务器只接受来自受信任域成员或特定组的域成员的网络连接。服务器隔离还可以为那些不是域成员的计算机提供连接，但是必须要有受信任 CA 颁发的计算机证书。

服务器和域隔离可以有效降低如下风险：

- 连接不受保护的无线网络和访问不要求应用层认证的服务器；
- 允许任何用户（包括物理连接网络）访问的服务器；
- 使用未认证计算机的认证用户。

服务器和域隔离只是安全性中的一层，不能防止如下危险：

- 认证用户使用了误用访问的认证计算机；
- 访问认证计算机的攻击者；
- 攻击认证计算机和其他网络计算机的蠕虫等病毒；
- 攻击者访问不受 IPSec 保护的服务器；
- 满足 IPSec 免除的未认证连接。

（4）IPSec 免除

在 Windows Server 2008 中默认情况下不要求 IPSec 认证，用户只有只有需要 IPSec 通信时才会需要免除。如果用户需要使用 IPSec 认证，需要为不支持 IPSec 认证的连接创建 IPSec 免除。通常情况下，管理员需要为如下用户创建 IPSec 免除：

- 最新配置的计算机，还没有对 IPSec 进行配置；
- 操作系统不支持 IPSec；
- Gutst 帐户。

应尽量减小免除的范围，通常只对不支持 IPSec 认证的连接批准免除。例如管理员可以在来宾无线接入上为某主机添加免除，使其能够来连接代理服务器和访问 Internet。很多基础服务器都需要使用 IPSec 免除：

- DHCP 服务器：DHCP 服务器需要通过 UDP 端口 68 来接收 DHCP 协商通信，但是不需要 IPSec；
- DNS 服务器：为允许客户端查找域控制器和其他网络资源，DNS 服务器必须允许 DNS 请求不使用 IPSec 通过 UDP 端口 53；
- Windows Internet 名称服务（WINS）服务器：如果客户端计算机需要 WINS 服务器，则需要为 WINS 请求所使用的 UDP 端口 137 创建一个免除；
- 域控制器：域控制器必须能够接受几种不受 IPSec 保护的不同的通信协议的连接。

每个创建的免除都是一个安全风险，必须仔细评估每个免除，然后采取措施降低安全风险。考虑攻击者使用免除访问受保护资源的所有可能性。例如如果允许了未经认证来宾用户访问代理服务器，就要确定该用户不能使用代理服务器访问其他受保护的资源，如内部文件服务器、



FTP 服务器等。

另外，用户还应该使用物理访问和网络访问保护（NAP）来保护使用免除的网络。例如如果需要为一台新配置的计算机创建一个免除，那么可以使用物理锁来限制网络访问。这将防止受 IPSec 保护的计算机去访问那些允许不受 IPSec 保护计算机访问的资源；降低了机密信息突然外泄给未认证计算机的危险，以及降低了来自未认证计算机的病毒攻击内网计算机的危险。

最后，还需要应用深度防御安全法则，不能仅仅依靠 IPSec 的安全性。如果内网的 Web 服务器需要 IPSec，那么用户还需要在 Web 应用程序中使用认证。同样地，如果使用 IPSec 加密 E-mail 服务器的通信，还需要启动应用层加密（例如，SSL 证书加密）。

如图 15.23 所示是 IPSec 连接策略在网络中的基本部署。域隔离应该用于限制连接到域成员的 IPSec 连接。

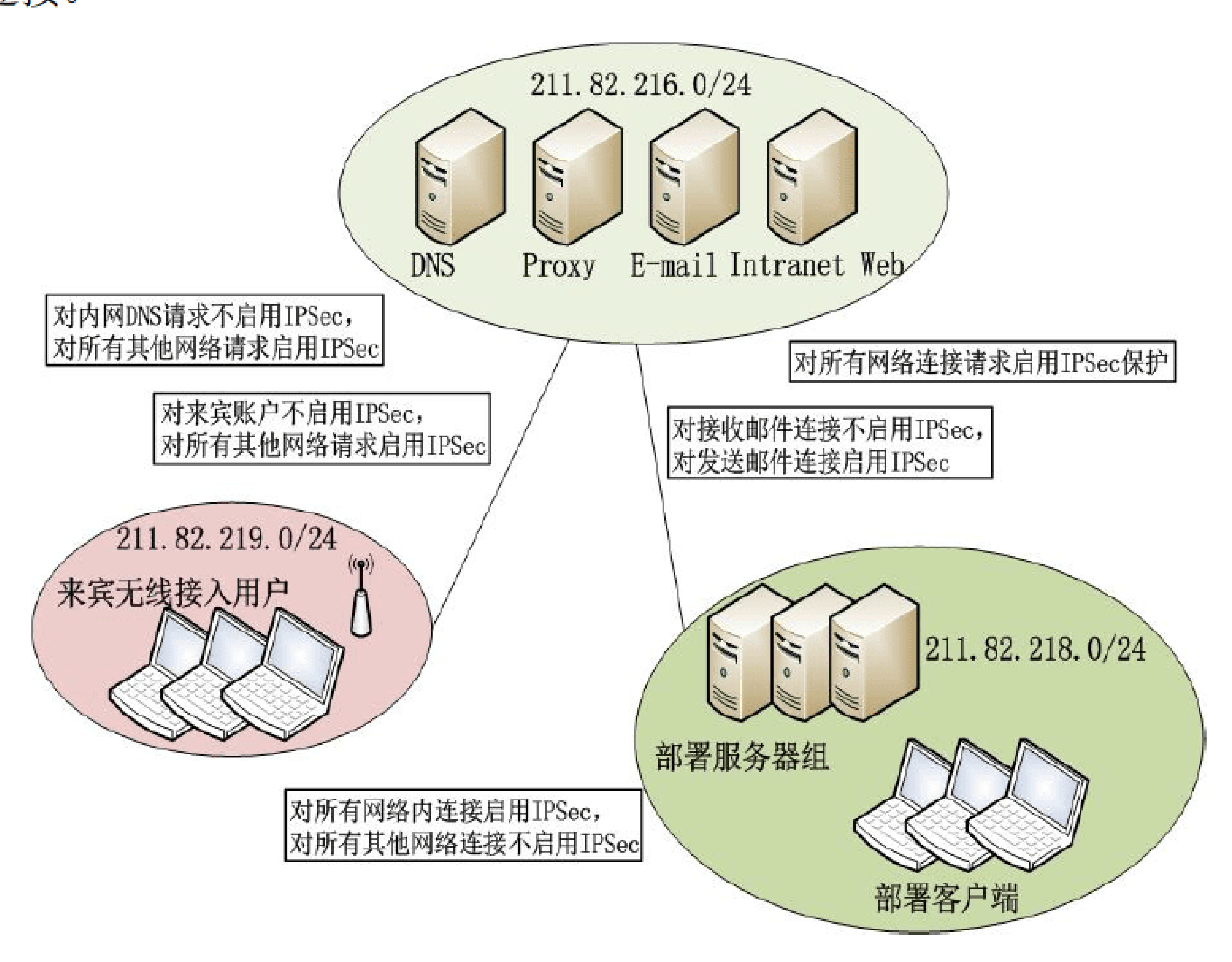


图 15.23 使用免除的隔离示例

2. 创建 IPSec 连接安全规则

01 打开“高级安全 Windows 防火墙”窗口，右击“连接安全规则”，选择快捷菜单中的“新规则”选项，启动“新建连接安全规则向导”，在“规则类型”对话框中，选择“自定义”单选按钮。单击“下一步”按钮，在“终结点”对话框中，选择“下列 IP 地址”单选按钮，单击“添加”按钮，即可添加终结点计算机，如图 15.24 所示。终结点是形成对等端连接的计算机或计算机组，可以是指定单个计算机，也可以是一个本地子网。

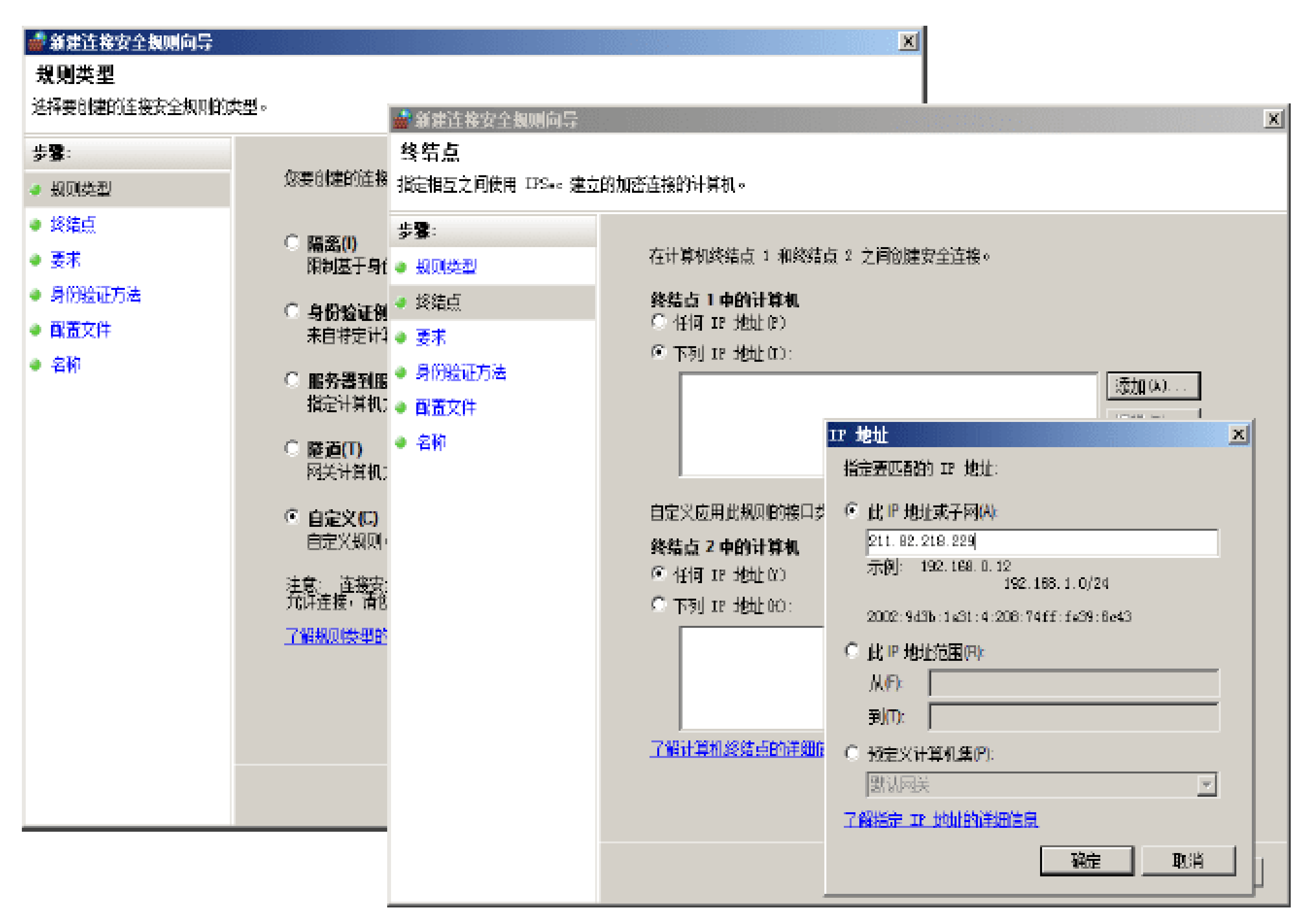


图 15.24　设置规则类型和终结点

注意　若要创建身份验证免除规则，只需要指定计算机或者一组或一个范围内的 IP 地址（计算机）并给出规则的名称和说明（可选）即可。即使对计算机免除身份验证，防火墙仍可能阻止这些计算机，除非防火墙规则已明确允许其连接。

02 单击“下一步”按钮，在“要求”对话框中，选择“入站和出站连接请求身份验证”单选按钮。单击“下一步”按钮，在“身份验证方法”对话框中，选择“默认值”单选按钮。除此之外，用户也可以选择“高级”单选按钮，重新定义自己需要的身份验证方法。单击“下一步”按钮，在“配置文件”对话框中，选择需要应用规则的配置文件，系统默认为全部选择，如图 15.25 所示。



图 15.25　设置身份验证要求、身份验证方法和配置文件类型

注意　
Kerberos V5 身份验证方法仅适用于 Windows 域环境，即只有计算机或用户帐户是域成员时，才可以使用该验证协议。

03 单击“下一步”按钮，显示如图 15.26 所示“名称”对话框，在“名称”和“描述”文本框中，分别输入规则名称和描述即可。最后单击“完成”按钮关闭向导，完成新规则的创建。



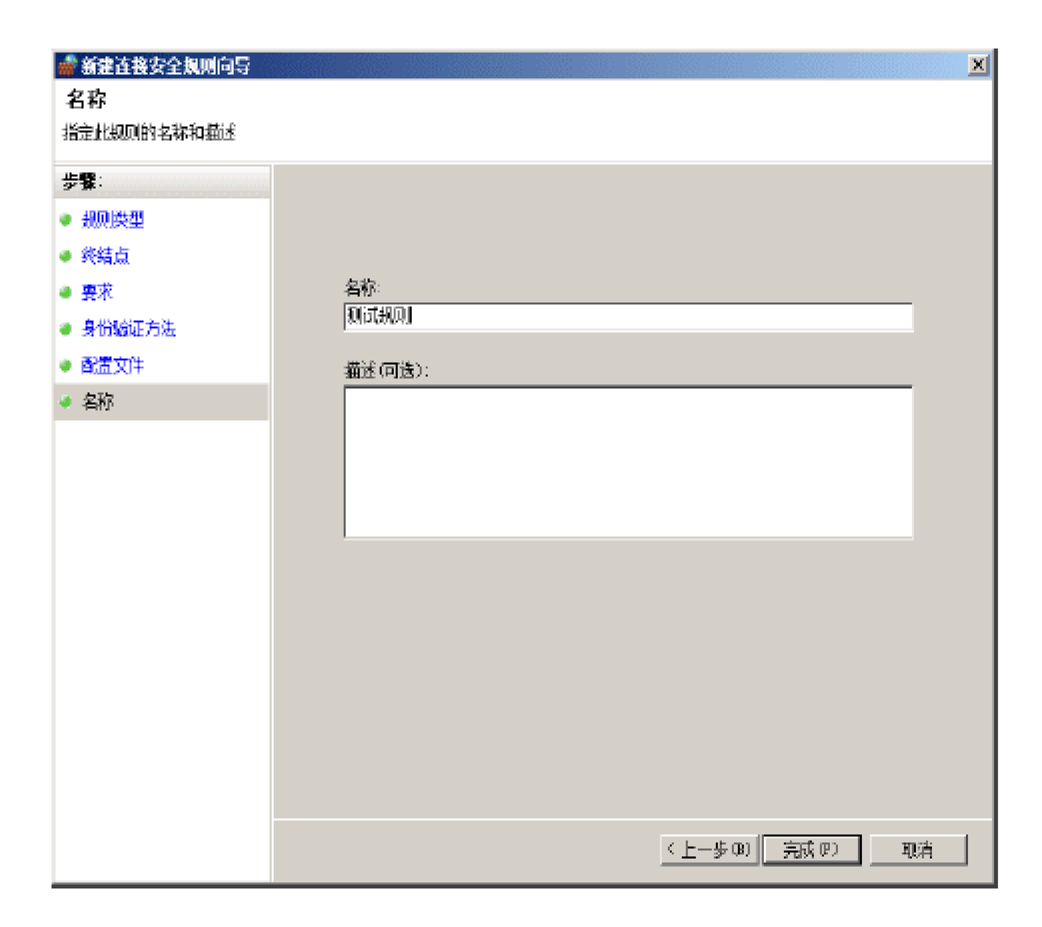


图 15.26　“名称”对话框

3. 配置域隔离

01 按照“配置常规防火墙设置”的步骤，在“高级安全 Windows 防火墙 属性”对话框中的“IPSec 设置”选项卡中，配置默认 IPSec 认证和加密要求。默认情况下，只有计算机认证是使用 Kerberos V5。为了更高的安全性，可以选择使用“计算机和用户认证”。

02 按照“添加 IPSec 连接安全规则”的步骤，为默认域 GPO 添加连接安全规则。

03 监视计算机保证 IPSec 连接和认证及加密都能够正常工作。此处可以参照后面讲到的“运行维护”。

04 按照“添加 IPSec 连接安全规则”的步骤，为不支持 IPSec 的免除计算机添加连接安全规则。该规则越详细越好，而且只能批准有限数量的这种计算机，允许它们访问尽量少的资源。在“新建连接安全规则向导”中，在“规则类型”对话框，选择“身份验证例外”选项。在“免除计算机”对话框，指定需要免除的计算机的 IP 地址。完成向导之后，编辑规则属性，然后选择“计算机”选项卡。如果只允许免除计算机访问有限的资源，那么将网络资源的 IP 地址输入到“终结点 1”中（“终结点 2”中列出的是免除计算机）。

05 为试验组中的计算机创建新的 GPO，然后按照“添加 IPSec 连接安全规则”的步骤，添加 IPSec 所要求的连接安全规则。在“规则类型”对话框，选择“隔离”。在“要求”对话框，选择“入站和出站连接要求身份认证”。对于服务器而言，向导页面的默认设置大多数环境下都是适用的。为了允许移动计算机连接其他网络的资源，需要将规则应用于“域配置文件”。

06 监视试验中的计算机，并保证它们能够正常工作和正常使用 IPSec。

07 通常需要扩展 IPSec 试验 GPO 的作用域，使更多的计算机能要求 IPSec。最后域中的所有计算机都要使用 IPSec 连接安全。

4. 配置服务器隔离

服务器隔离配置步骤和域隔离相似。对于客户端计算机的安全配置，两种方法基本相同，但是对于服务器来说，服务器隔离只要求对入站连接进行安全配置，而域隔离是通过创建免除优先来进行安全配置。

服务器隔离使用的是 Kerberos V5 认证或计算机证书的认证方式。如果用户使用的是计算机证书认证，那么需要满足如下要求之一：

- 从公有 CA 处购买证书：从 Windows 信任的 CA 处购买的证书，用于 IPSec 通信的效果

是很理想的。客户端计算机同样也需要证书；

- 使用内部 CA 产生证书：用户可以通过内网 CA（如 Windows Server 2008 活动目录证书服务）产生自己的证书。服务器和客户端都要使用该证书，并且所有计算机都要信任该证书。

5. 配置 ICMP 免除

管理员经常使用 ICMP 协议中的“ping”命令来确认网络运行状态。如果服务器的 IPSec 阻止“ping”命令，管理员就无法正常使用该工具。因此，需要在 IPSec 安全连接规则中创建 ICMP 免除。

在高级安全 Windows 防火墙控制台中，右击“高级安全 Windows 防火墙”，在弹出的快捷菜单中选择“属性”选项，打开“高级安全 Windows 防火墙-本地组策略对象 属性”对话框，选择“IPSec 设置”选项卡（如图 15.27 所示），在“从 IPSec 免除 ICMP”菜单中，选择“是”，然后单击“确定”按钮即可。



图 15.27 “IPSec 设置”选项卡

15.3 使用组策略配置 Windows 防火墙

在中小型网络环境中，通过使用 Active Directory 和组策略，可以集中配置 Windows 防火墙的设置，并将这些设置应用到所有 Windows XP SP2 客户端计算机。用户可以在 Windows Vista 和 Windows Server 2008 计算机的组策略控制台中，可以通过如下两种方式配置和管理高级安全 Windows 防火墙：

- 计算机配置\Windows 设置\安全设置\高级安全 Windows 防火墙\高级安全 Windows 防火墙：这种节点设置主要应用于 Windows Vista 和 Windows Server 2008。建议用户使用这种方式，因为这里可以提供更加详细的防火墙规则配置，并且允许用户配置新的认证类型和新的加密选项；
- 计算机配置\管理面板\网络\网路连接\Windows 防火墙：这种节点设置主要应用于



Windows XP、Windows Server 2003、Windows Vista 和 Windows Server 2008。这种方法要比上面那种缺少灵活性；但是，可以应用于所有版本的 Windows 防火墙。如果在 Windows Vista 中使用的不是最新的 IPSec 功能，可以使用这种方式配置所有客户端。

15.3.1　创建组策略

为了到达最好的效果，需要为 Windows XP/Windows Server 2003/Windows Vista/Windows Server 2008 创建单独的组策略，然后使用 WMI 请求定位组策略到运行适当的 Windows 版本的计算机。

01 以具有域管理员权限的用户登录到域控制器，依次选择“开始”→“管理工具”→“组策略管理”选项，打开“组策略管理”窗口。依次展开“林”→“域”→“coolpen.net”选项，右击新建策略应用到的组织单位，选择快捷菜单中的“在这个域中创建 GPO 并在此处链接”选项，显示如图 15.28 所示“新建 GPO”对话框，在“名称”文本框中，输入希望使用的策略名称，如 Windows 防火墙。

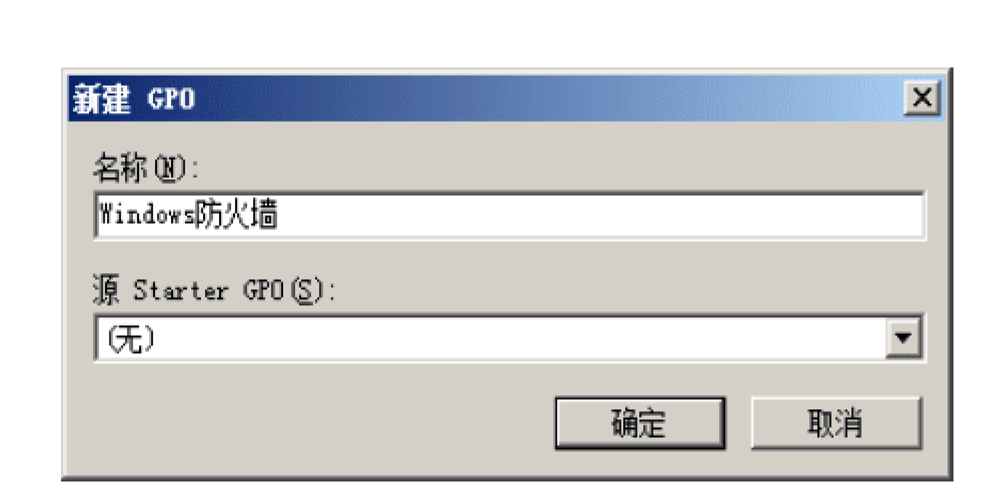


图 15.28　“新建 GPO”对话框

02 单击“确定”按钮，返回如图 15.29 所示“组策略管理”窗口。右击创建成功的“Windows 防火墙”，选择快捷菜单中的“编辑”选项，显示“组策略管理编辑器”窗口，依次展开“计算机配置”→“策略”→“管理模板”→“网络”→“网络连接”→“Windows 防火墙”选项，即可开始编辑 Windows 防火墙相关的策略设置。

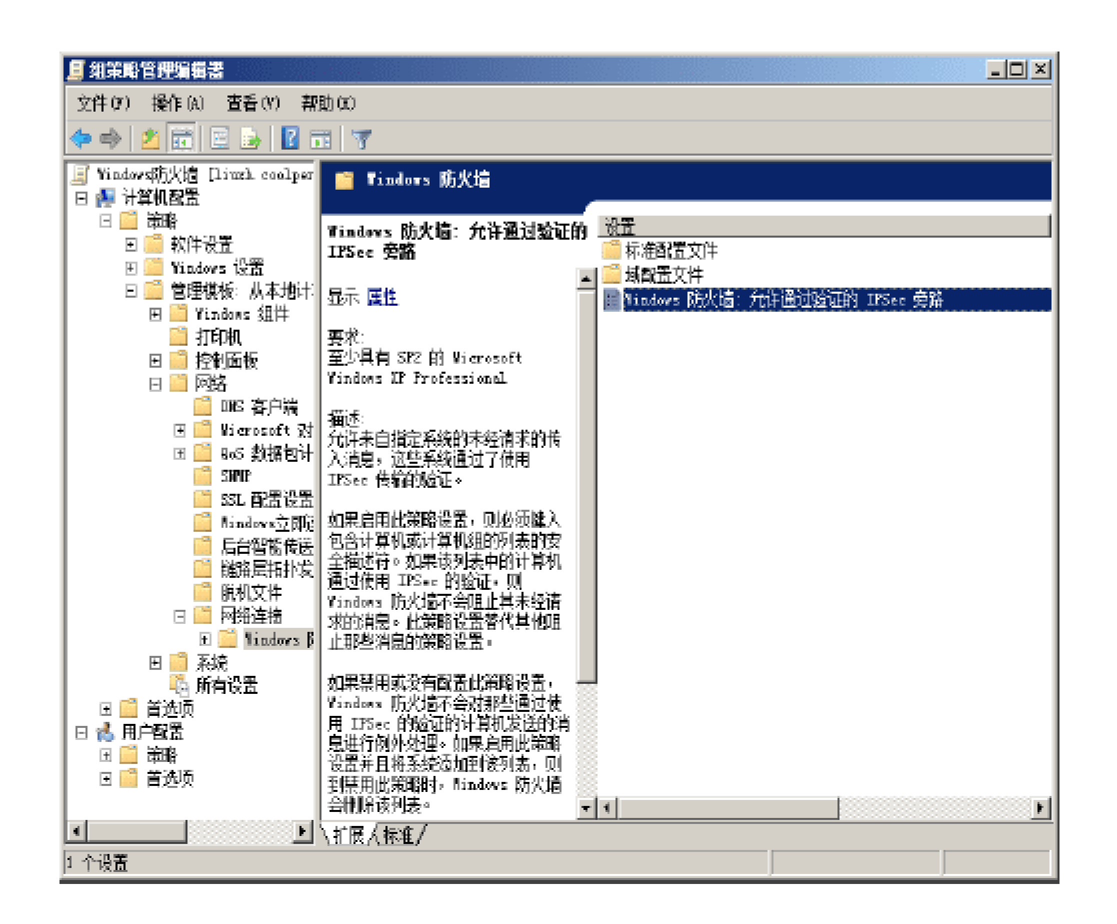


图 15.29　“组策略管理编辑器”窗口

15.3.2　设置 Windows 防火墙：允许通过验证的 IPSec 旁路

该策略将允许来自指定系统的未经请求的传入消息，如果启用该策略设置，必须输入包含计算机或计算机组的列表的安全描述符。如果列表上的计算机通过使用 IPSec 的验证，Windows 防火墙不会阻止未经请求的消息。如果禁用或不配置该策略设置，Windows 防火墙不会对计算机发送的消息进行例外处理，即使计算机通过了 IPSec 的验证。

01 在组策略对象编辑器的控制台树中，选择“计算机配置”→“管理模板”→“网络”→“网络连接”→“Windows 防火墙”选项。显示如图 15.30 所示组策略中的 Windows 防火墙选项。

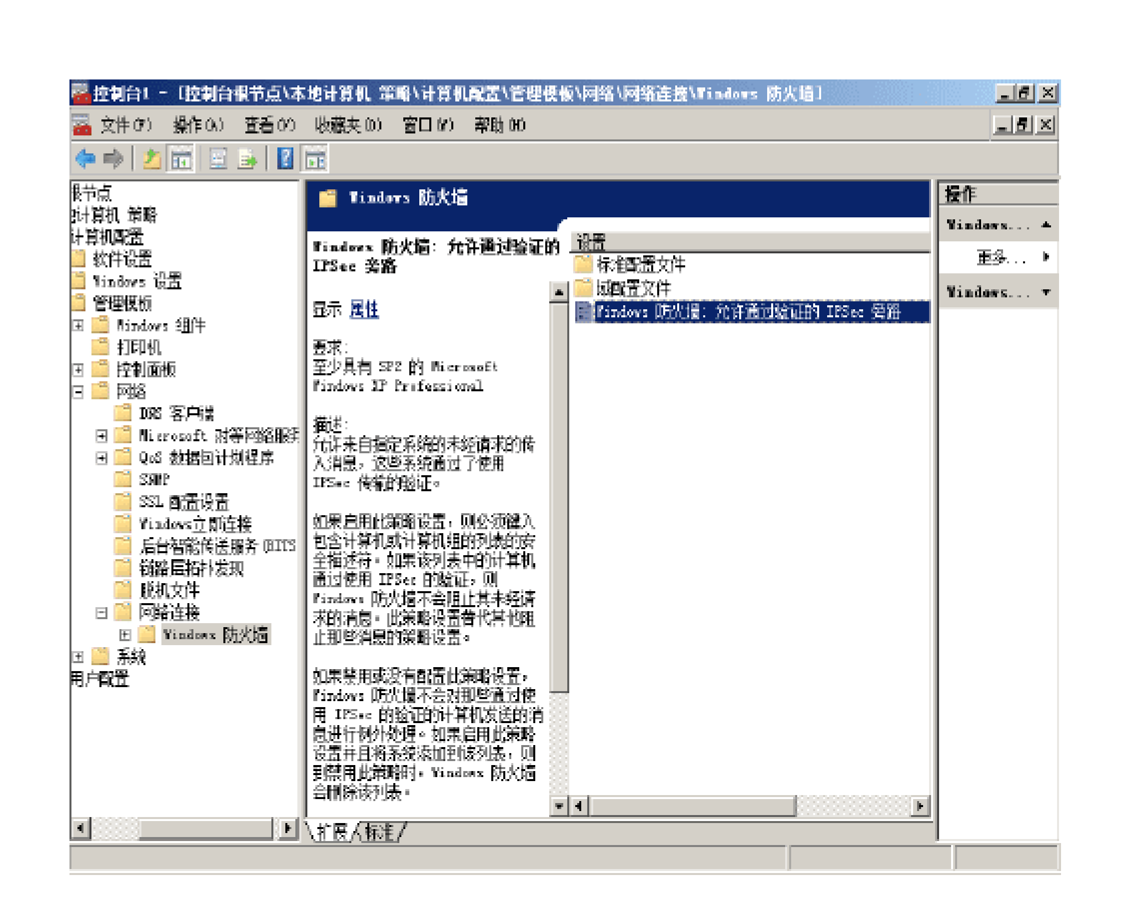


图 15.30 组策略中的 Windows 防火墙选项

02 双击“Windows 防火墙：允许通过验证的 IPSec 旁路”策略，显示如图 15.31 所示“Windows 防火墙：允许通过验证的 IPSec 旁路 属性”对话框。根据需要选中“已启用”或者“已禁止”单选按钮，即可完成策略的设置。然后单击“确定”按钮。

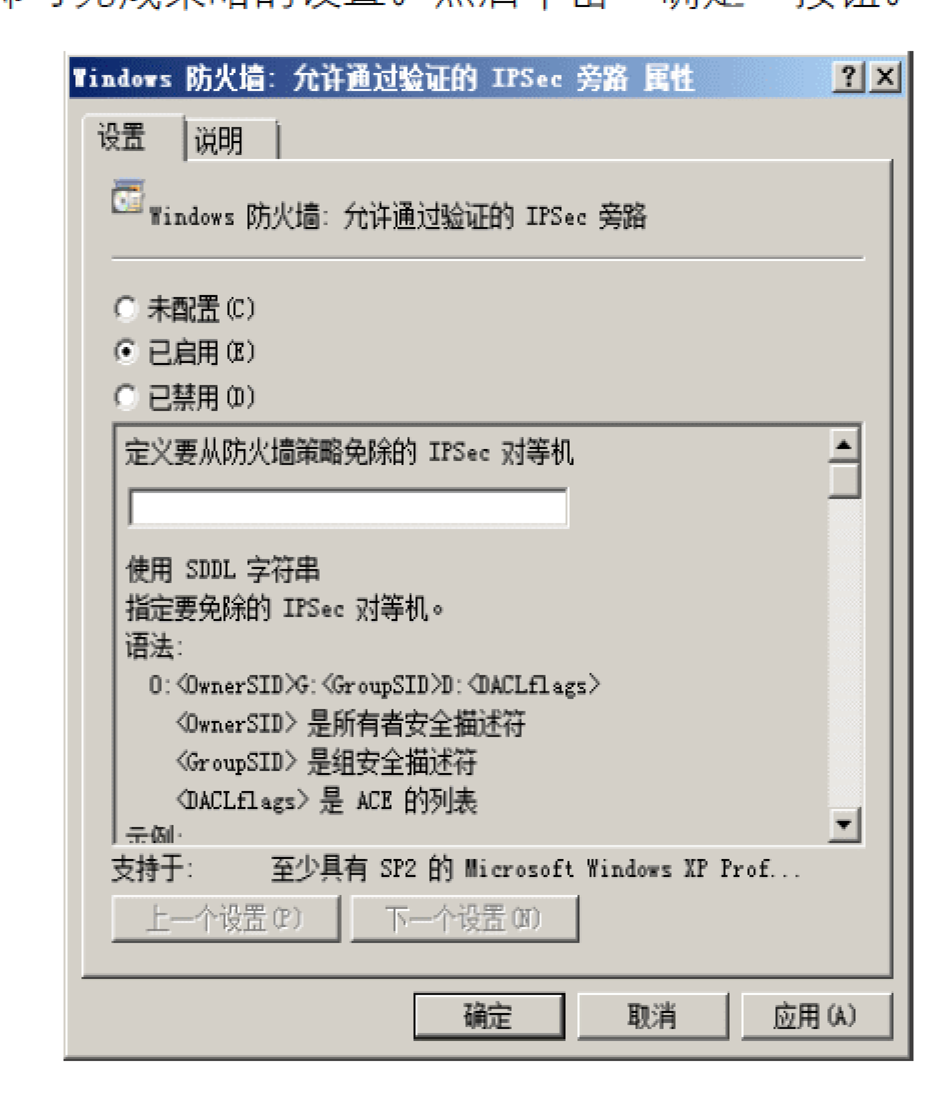


图 15.31 “Windows 防火墙：允许通过验证的 IPSec 旁路属性”对话框

> 提示 “允许通过验证的 IPSec 旁路”设置如下：
> - 未配置：此 GPO 不会更改 Windows 防火墙的当前配置；
> - 已启用：Windows 防火墙不会处理受 IPSec 保护的通信，除非是来自策略中列出的用户或组；
> - 已禁用：Windows 防火墙将处理受 IPSec 保护的通信。

15.3.3 标准配置文件/域配置文件

Windows 防火墙配置文件分为：标准配置文件和域配置文件。标准配置文件是基于本地计算机的 Windows 防火墙配置；域配置文件是基于 AD 的网络防火墙配置。标准配置文件和域配置文件下的子策略所完成的功能，与“Windows 防火墙”设置所完成的功能是相同。

这里以域配置文件为例，介绍如何在组策略下配置 Windows 防火墙。打开组策略控制台，依次展开“计算机配置”→“Windows 设置”→“管理模板”→“网络”→“网络连接”→“Windows 防火墙”→“域配置文件”选项，在右侧列表中显示 Windows 防火墙域配置文件策略中的所有子策略，如图 15.32 所示。

例如，配置“Windows 防火墙：允许本地程序例外”策略。如果启用该策略设置，将允许用户在 Windows 防火墙组件中向本地程序中添加例外列表。双击右侧窗口中的“Windows



防火墙：允许本地程序例外”策略，打开“Windows 防火墙：允许本地程序例外 属性”对话框，如图 15.33 所示。根据需要选择“已启用”单选按钮，即可启用该策略。

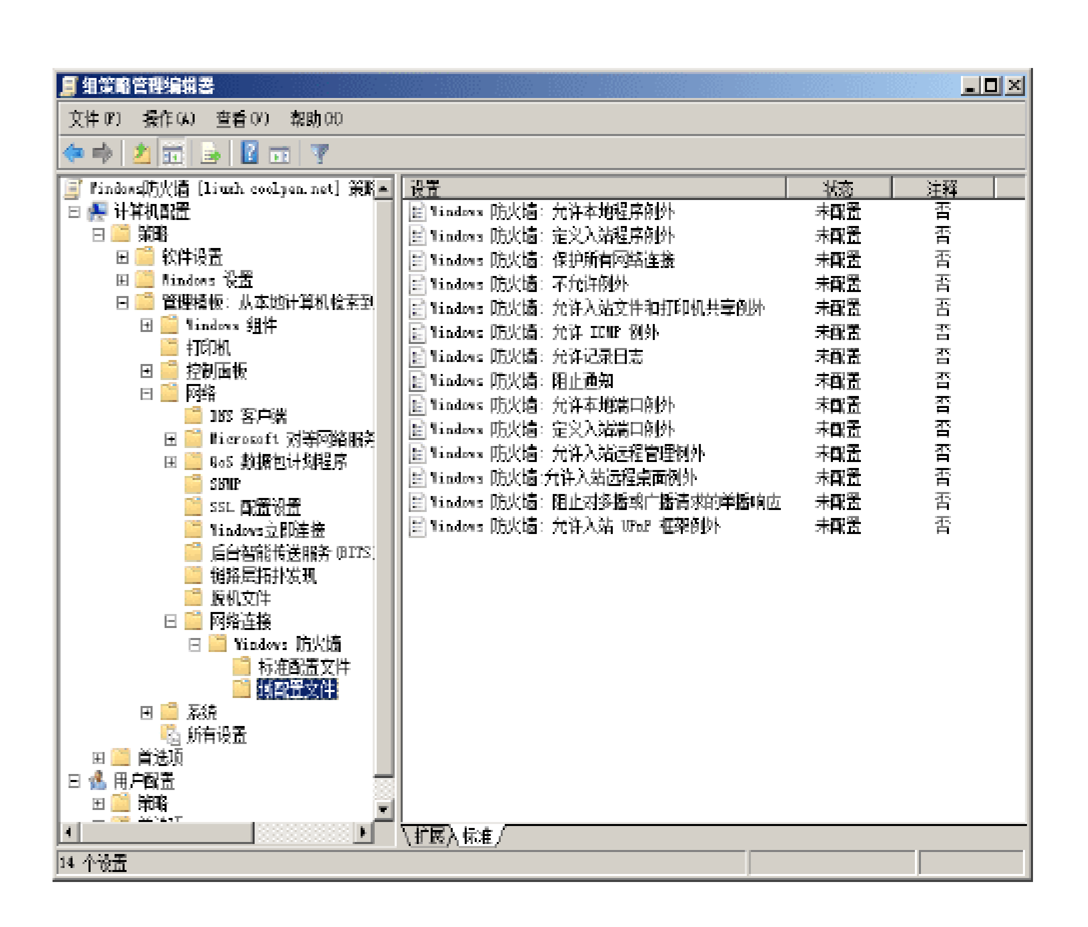


图 15.32　域配置文件窗口

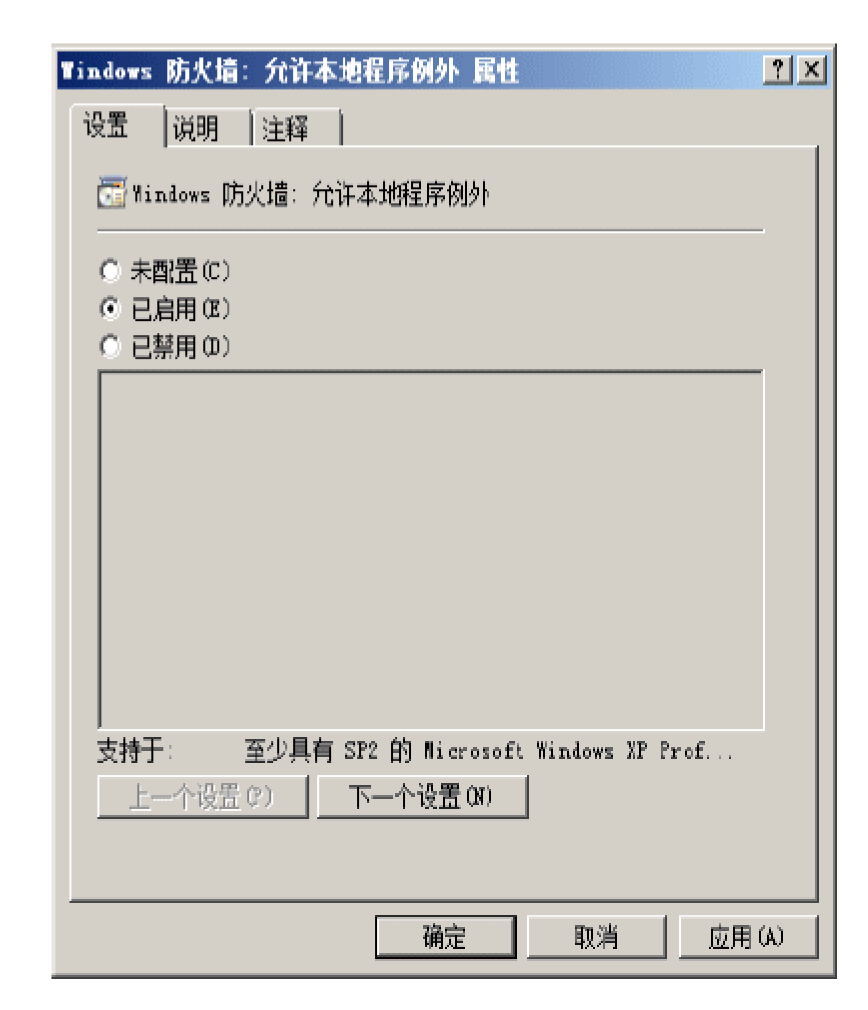


图 15.33　“Windows 防火墙：允许本地程序例外 属性”对话框

在中小型企业网络中，推荐用户按照表 15.2 中的推荐值，部署 Windows 防火墙标准配置文件和域配置文件。

表 15.2　小型或中型企业的 Windows 防火墙组策略推荐配置

设置	描述	标准配置文件	域配置文件
允许本地程序例外	启用程序例外的本地配置	已禁用	已禁用，除非需要本地管理员在本地配置程序例外
定义入站程序例外	按照程序文件名定义例外通信	如果网络上的计算机运行 WindowsXP SP2，则启用和配置由其使用的程序	如果网络上的计算机运行 WindowsXP SP2，则启用和配置由其使用的程序
保护所有网络连接	指定为所有网络连接启用 Windows 防火墙	已启用	已启用
不允许例外	指定放弃所有进入的垃圾通信，包括例外通信	已启用，除非您必须配置程序例外	未配置
允许入站文件和打印机共享例外	指定是否允许文件和打印机共享通信	已禁用	已禁用，除非运行 WindowsXP SP2 的计算机正在共享本地资源
允许 ICMP 例外	指定允许的 ICMP 消息类型	已禁用	已禁用，除非希望使用 ping 命令排除故障
允许记录日志	允许通信日志和配置日志文件设置	未配置	未配置
阻止通知	禁用通知	已禁用	已禁用
允许本地端口例外	启用端口例外的本地配置	已禁用	已禁用

（续表）

设置	描述	标准配置文件	域配置文件
定义入站端口例外	按照 TCP 和 UDP 指定例外通信	已禁用	已禁用
允许入站远程管理例外	允许使用工具进行远程配置	已禁用	已禁用，除非希望能够使用 MMC 管理单元远程管理您的计算机
允许入站桌面例外	指定计算机是否可以接受基于远程桌面的连接请求	已启用	已启用
阻止对多播或广播请求的单播响应	放弃针对多播或广播请求消息而收到的单播数据包	已启用	已启用
允许入站 UPnP 框架例外	指定计算机是否可以接收垃圾 UPnP 消息	已禁用	已禁用

15.3.4 合理部署标准配置文件/域配置文件示例

1. 定义入站端口例外策略

如果启用该策略设置，可以查看和更改由组策略定义的端口例外列表。如果禁用该策略设置，由组策略定义的端口例外列表将被删除，但其他策略设置可以继续打开或禁用端口。此时，如果存在本地端口的例外列表，将会被 Windows 防火墙忽略掉，除非用户启用了“Windows 防火墙：允许本地端口例外”策略设置。如果不配置该策略设置，Windows 防火墙只会使用由“Windows 防火墙”组件定义的本地端口例外列表。

01 在“域配置文件”设置区域中，双击“Windows 防火墙：定义入站端口例外”选项。显示如图 15.34 所示“Windows 防火墙：定义入站端口例外 属性”对话框。

02 选择“已启用”单选按钮，单击“显示”按钮，打开“显示内容”对话框。单击“添加”按钮，显示如图 15.35 所示“添加项目”对话框。输入要阻止或启用的端口的相关信息。使用以下语法：

port：transport：scope：status：name

提示



port 是端口号码，transport 是 TCP 或 UDP，scope 是*（用于所有计算机）或允许访问端口的计算机列表，status 是已启用或已禁用，name 是用作此条目标签的文本字符串。此实例名为 text，并为所有连接启用 TCP 端口 80。



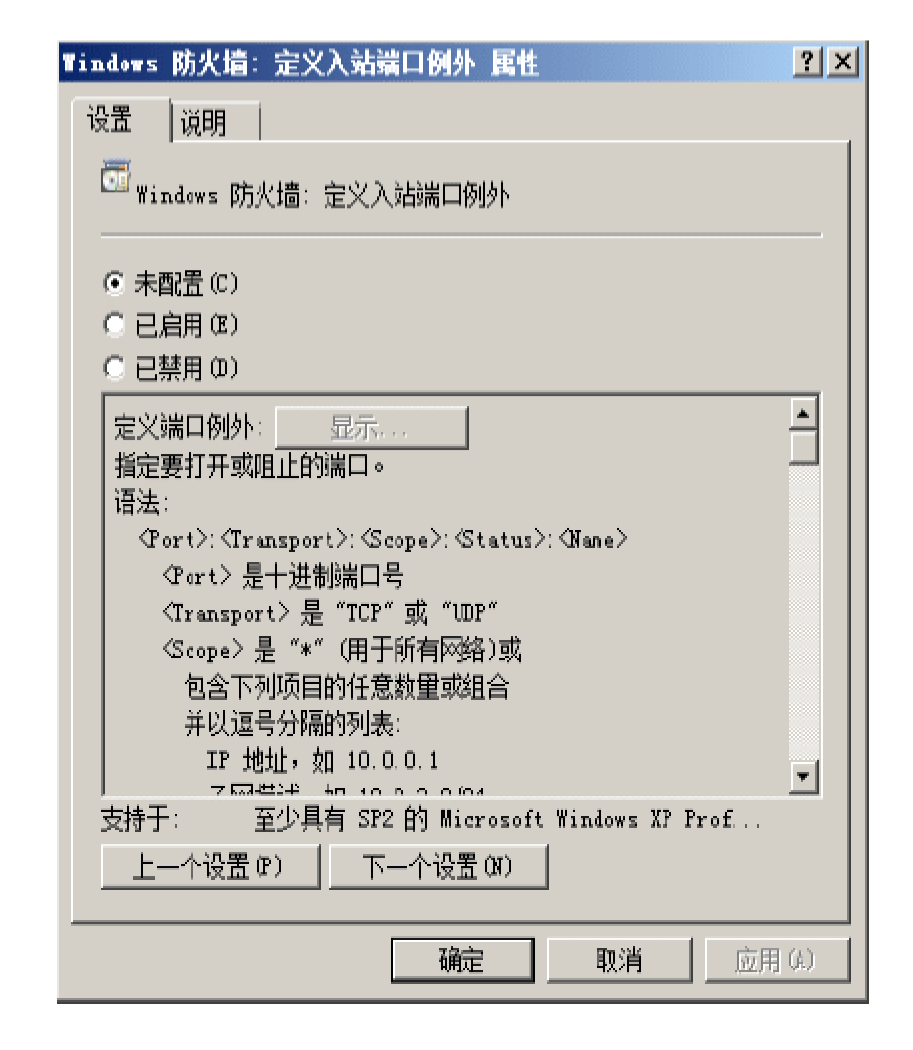


图 15.34　“Windows 防火墙：定义入站端口例外 属性”对话框



图 15.35　添加项目

03 依次单击“确定”按钮，关闭“Windows 防火墙：定义端口例外 属性”对话框，保存设置即可。

2. 启用入站程序例外策略

如果启用了该策略设置，可以查看和更改由组策略定义的程序例外列表。如果将一个程序添加到此列表并将其状态设置为“已启用”，此程序就可以在要求 Windows 防火墙打开的任何端口上，接受到未经请求的传入消息，即使此端口被其他策略设置阻止。如果禁用该策略设置，由组策略定义的程序例外列表将被删除。如果想继续使用本地的程序例外列表，则必须启用“Windows 防火墙：允许本地程序例外”策略设置。

01 在“域配置文件”设置区域中，双击“Windows 防火墙：定义入站程序例外”选项。显示如图 15.36 所示“Windows 防火墙：定义入站程序例外 属性”对话框。

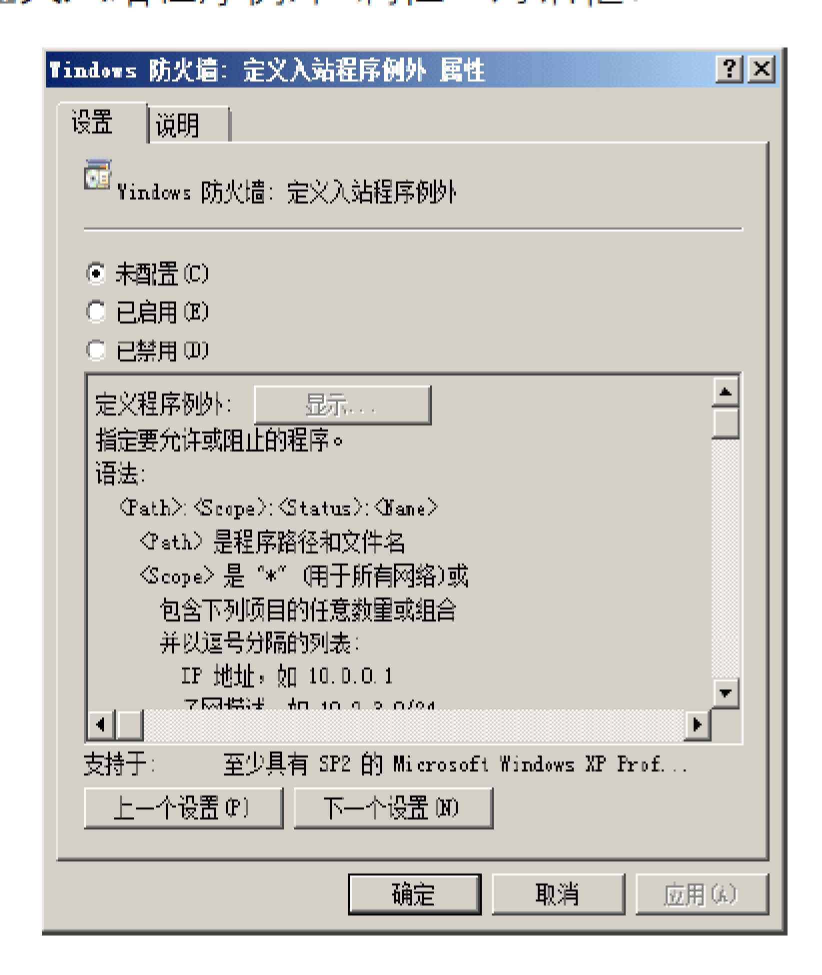


图 15.36　“Windows 防火墙：定义程序例外 属性”对话框

02 选择“已启用”单选按钮，单击“显示”按钮，打开“显示内容”对话框，单击“添加”按钮，显示如图 15.37 所示“添加项目”对话框。输入要阻止或启用程序的相关信息。使用以下语法：

path：scope：status：name

提示 path 是程序路径和文件名，scope 是*（用于所有计算机）或允许访问程序的计算机列表，status 是已启用或已禁用，name 是用作此条目标签的文本字符串。

03 此实例名为 MSN，为所有连接启用 WindowsLive 程序：D：\software\wlsetup-web.exe。输入完成后，单击“确定”按钮，将其添加到“显示内容”对话框中即可。

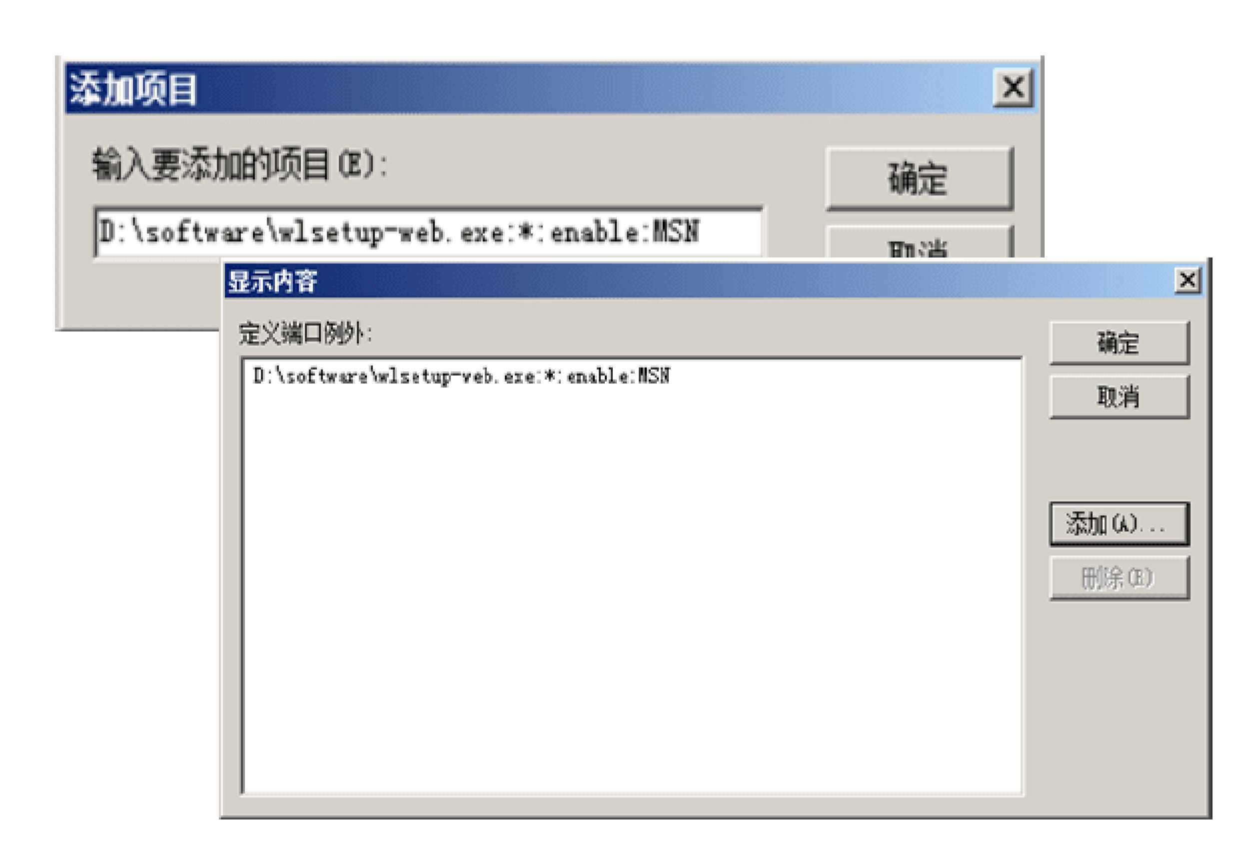


图 15.37 “添加项目”对话框

04 依次单击“确定”按钮，保存设置即可。



注意 如果输入无效的定义字符串，Windows 防火墙不会检查其是否存在错误。利用这个特点，可以将还没有安装的程序添加进来。需要注意的是，可以为一个程序创建作用域或状态值相互冲突的多个项目。Windows 防火墙只会为正在运行并在监听传入消息的程序打开端口，如果此程序没有运行，或正在运行但不在监听消息，Windows 防火墙都不会为其打开任何端口。

3. 允许 ICMP 例外策略

如果启用该策略设置，必须指定 Windows 防火墙允许本地计算机发送和接收的 ICMP 消息类型。如果禁用该策略设置，Windows 防火墙会阻止所有未经请求的传入 ICMP 消息类型和列出的传出 ICMP 消息类型。因此，使用阻止的 ICMP 消息的工具将无法向此计算机发送或从此计算机接收这些消息。如果不配置该策略设置，Windows 防火墙与禁用该策略的表现是相同。

01 双击“Windows 防火墙：允许 ICMP 例外”选项，显示如图 15.38 所示“Windows 防火墙：允许 ICMP 例外 属性”对话框。选择“已启用”单选按钮，选择要启用的适当 ICMP 例外。

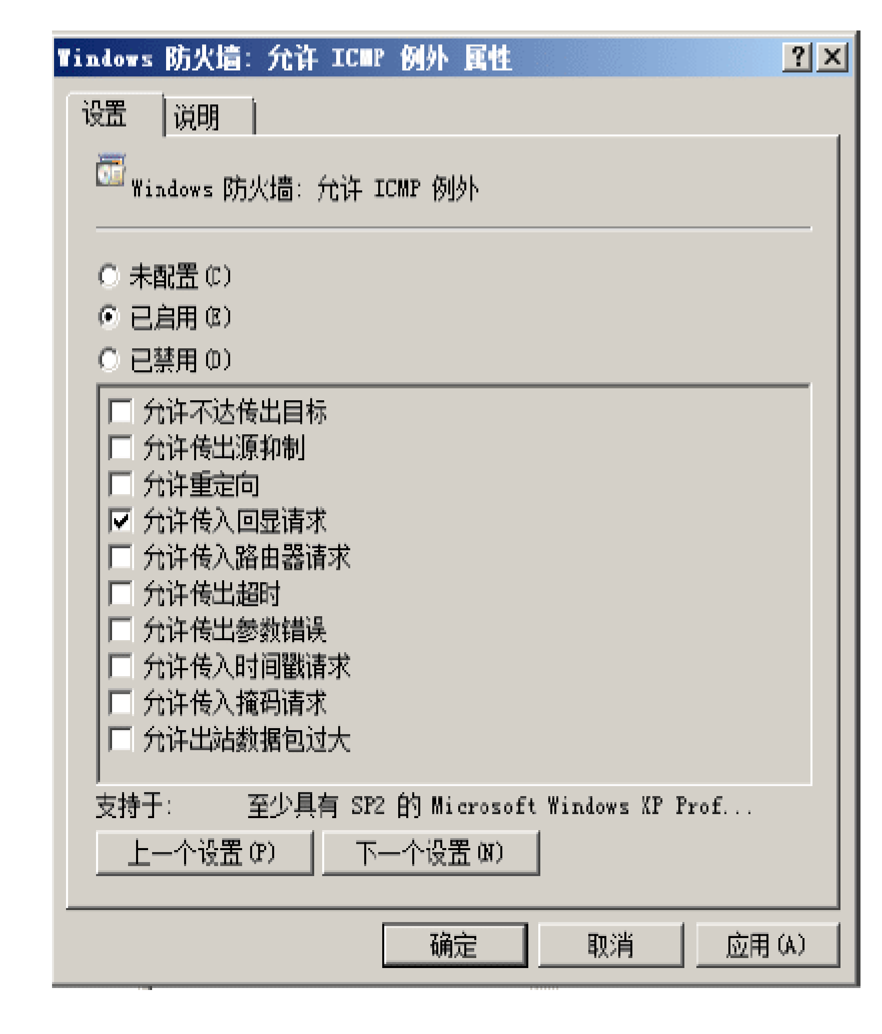


图 15.38 “Windows 防火墙：允许 ICMP 例外 属性”对话框



02 单击“确定”按钮，关闭“Windows 防火墙：允许 ICMP 例外 属性”对话框。

4. 允许记录日志策略

该策略用于配置，是否允许 Windows 防火墙记录有关其接收的未经请求的传入消息的信息。如果启用该策略设置，Windows 防火墙将信息写入日志文件。需要注意的是，必须提供日志文件的名称、位置和大小上限等信息。必须同时指定是否记录有关防火墙阻止（丢弃）的传入消息的信息，及成功的传入和传出连接的消息，Windows 防火墙不会提供记录成功的传入消息的方法。

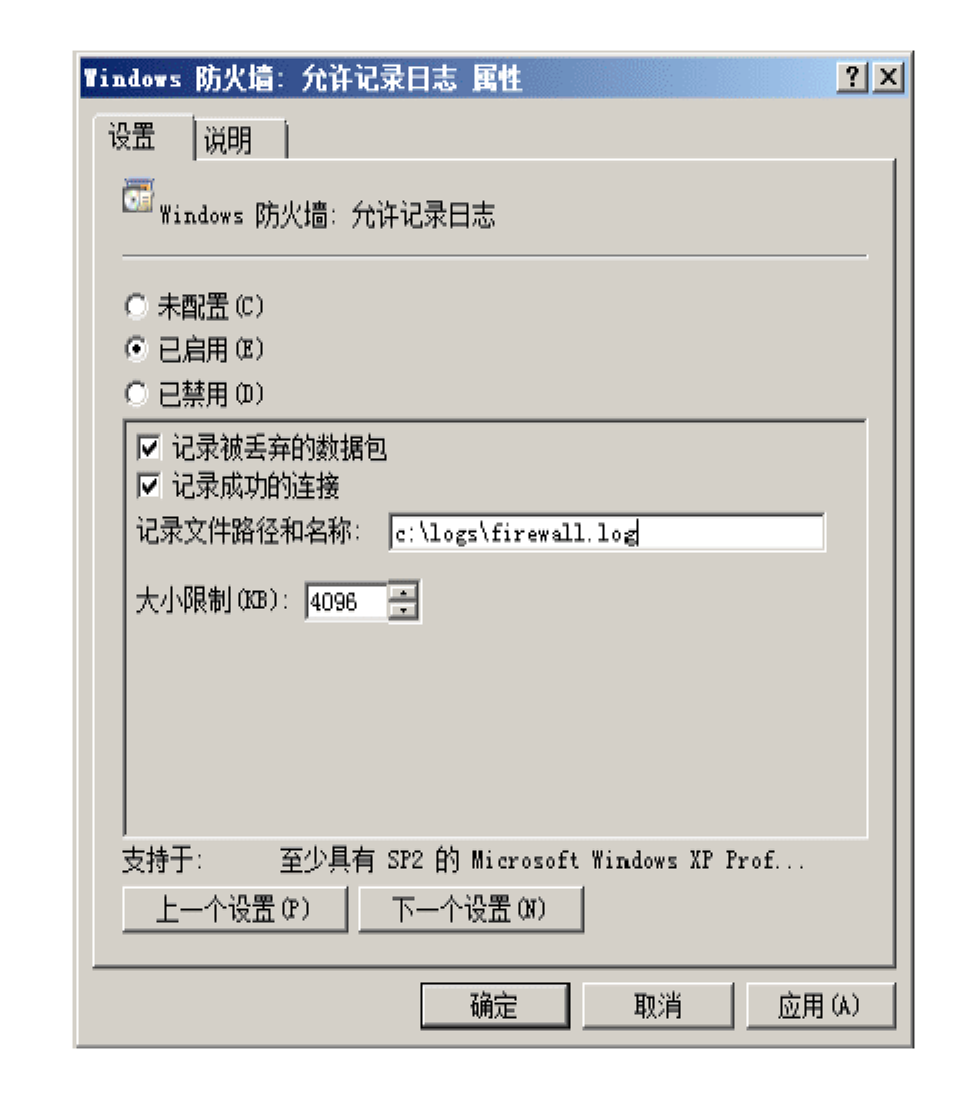


图 15.39 “Windows 防火墙：允许记录日志 属性”对话框

01 在“域配置文件”设置区域中，双击“Windows 防火墙：允许记录日志”选项，显示“Windows 防火墙：允许记录日志 属性”对话框。选择“已启用”单选按钮，选中“记录被丢弃的数据包”和“记录成功的连接”复选框，输入日志文件路径和名称，保留默认日志文件大小，显示如图 15.39 所示“Windows 防火墙：允许记录日志 属性”对话框，然后单击“确定”按钮。



注意　必须确保将日志文件保存到一个安全的位置，以免遭受任何意外或故意修改。

02 完成对 Windows 防火墙设置的更改后，关闭控制台。



注意　关闭控制台时，将会提示保存控制台。无论是否保存控制台，GPO 设置都会得到保存。

15.4　使用命令行配置 Windows 防火墙

对于初级管理员而言，控制台和组策略方式比较适用，但是对于管理技能丰富的高级管理员而言，前两种方式略显麻烦，命令行管理方式更加简便、快捷、高效。在 Windows Server 2008 系统中，管理员可以使用全新的 netsh advfirewall>命令环境，配置和管理“高级安全 Windows 防火墙”。

15.4.1 常用命令介绍

netsh advfirewall 是 netsh 命令的一个子命令，不仅继承了 netsh>环境下的部分子命令，还包含一些专用的命令选项。netsh advfirewall 从 netsh>环境下继承来的子命令如下：

- ..——移到上一层上下文级；
- Abort——丢弃在脱机模式下所做的更改；
- Add——在项目列表上添加一个配置项目；
- Advfirewall——更改到“netsh advfirewall”上下文；
- Alias——添加一个别名；
- Bridge——更改到“netsh bridge”上下文；
- Bye——退出程序；
- Commit——提交在脱机模式中所做的更改；
- Delete——在项目列表上删除一个配置项目；
- Dhcpclient——更改到“netsh dhcpclient”上下文；
- Exit——退出程序；
- Firewall——更改到“netsh firewall”上下文；
- http——更改到“netsh http”上下文；
- Interface——更改到“netsh interface”上下文；
- IPSec——更改到“netsh IPSec”上下文；
- Lan——更改到“netsh lan”上下文；
- Nap——更改到“netsh nap”上下文；
- Netio——更改到“netsh netio”上下文；
- Offline——将当前模式设置成脱机；
- Online——将当前模式设置成联机；
- Popd——从堆栈上打开一个上下文；
- Pushd——将当前上下文放入堆栈；
- Quit——退出程序；
- Ras——更改到“netsh ras”上下文；
- Rpc——更改到“netsh rpc”上下文；
- Set——更新配置设置；
- Show——显示信息；
- Unalias——删除一个别名；
- Winhttp——更改到“netsh winhttp”上下文；
- Winsock——更改到“netsh winsock”上下文；
- Wlan——更改到“netsh wlan”上下文。

除上述继承选项外，netsh advfirewall 命令还支持如下选项和子命令：



- ?——显示命令列表；
- Consec——更改到“netsh advfirewall consec”上下文；
- Dump——显示一个配置脚本；
- Export——将当前策略导出到文件；
- Firewall——更改到“netsh advfirewall firewall”上下文；
- Help——显示命令列表；
- Import——将策略文件导入当前策略存储；
- Monitor——更改到“netsh advfirewall monitor”上下文；
- Reset——将策略重置为默认全新策略；
- Set——设置每个配置文件或全局设置；
- Show——显示配置文件或全局属性。

1. Help 命令

Help 命令是最有用，也是最好用的命令。任何时候输入“?”命令，都会看到和上下文相关的所有选项，既简单又方便。

注意　如果在命令提示符中直接输入“? ”，将会显示是不可运行的程序或批处理文件。出现这种情况时，可以直接输入“help”命令，再按下回车键。即可显示详细信息作为参考。

---

2. Consec（连接安全规则）命令

Consec 是连接安全规则命令，这个连接规则可以创建两个系统之间的 IPSec VPN。换言之，Consec 规则能够加强通过防火墙的通信的安全性，而不仅仅是限制或过滤它。Consec 环境中支持的命令包括：

- add 命令添加新连接安全规则；
- delete 命令删除所有匹配的连接安全规则；
- dump 命令显示一个配置脚本；
- help 命令显示命令列表；
- set 命令为现有规则的属性设置新值；
- show 命令显示指定的连接安全规则。

3. Export 命令

Export 命令可以导出防火墙当前所有的配置到一个文件中。这个命令非常有用，可以备份所有的配置到文件中，如果对已经做出的配置不满意，可以随时使用这个文件恢复到修改前的状态。

4. Import 命令

Import 命令可以从一个文件中导入防火墙的配置。这个命令可以把之前使用 Export 命令导出的防火墙配置再恢复回去。

5. Firewall 命令

使用 Firewall 命令既可以增加新的入站和出站规则到防火墙中，还可以修改防火墙中的规则。在 firewall 上下文命令中，支持的命令包括：

- add 命令添加新入站或出站防火墙规则；
- delete 命令删除所有匹配入站规则；
- dump 显示一个配置脚本；
- help 命令显示命令列表；
- set 命令为现有规则的属性设置新值；
- show 命令将显示指定的防火墙规则。

6. Reset 命令

Reset 命令可以重新设置防火墙策略到默认策略状态。使用这个命令时务必谨慎，因为一旦输入这个命令并按下回车后，它将不再确认是否真要重设，直接恢复防火墙的策略。

7. Set 命令

Set 命令允许修改防火墙的不同设置状态，该命令环境下支持的命令包括：

- set allprofiles 在所有配置文件中的设置属性；
- set currentprofile 在活动配置文件中设置属性；
- set domainprofile 在域配置文件中设置属性；
- set global 设置全局属性；
- set privateprofile 在专用配置文件中设置属性；
- set publicprofile 设置公用配置文件中的属性。

15.4.2 命令行配置示例

1. 使用默认值为域隔离添加规则

为当前域中所有客户端添加隔离规则，名称为 coolpen，身份验证方式为：入站要求身份验证，出站请求身份验证。在命令提示符窗口中输入如下命令：

```
    netsh advfirewall consec add rule name="coolpen" endpoint1=any endpoint2=any
action=requireinrequestout
```

回车执行，成功完成后显示如图 15.40 所示结果。“确定”表示创建成功。

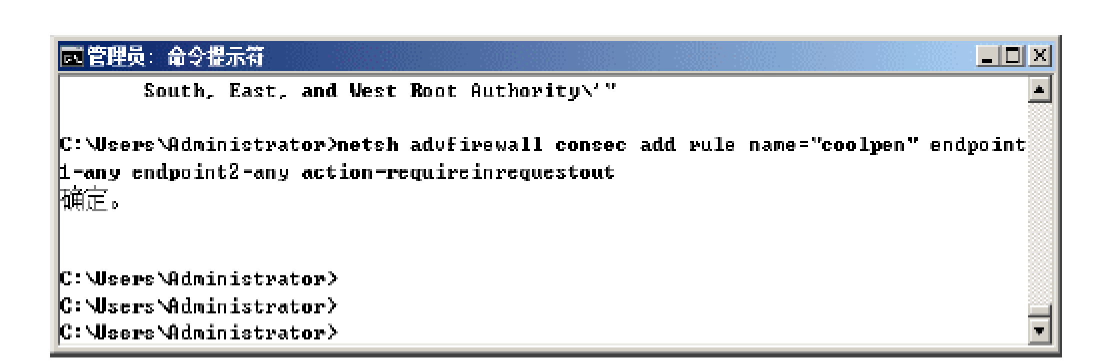


图 15.40 创建域隔离规则

为检验规则详细配置信息，可以继续输入如下命令：

```
netsh advfirewall consec show rule coolpen
```

回车执行，显示如图 15.41 所示结果。

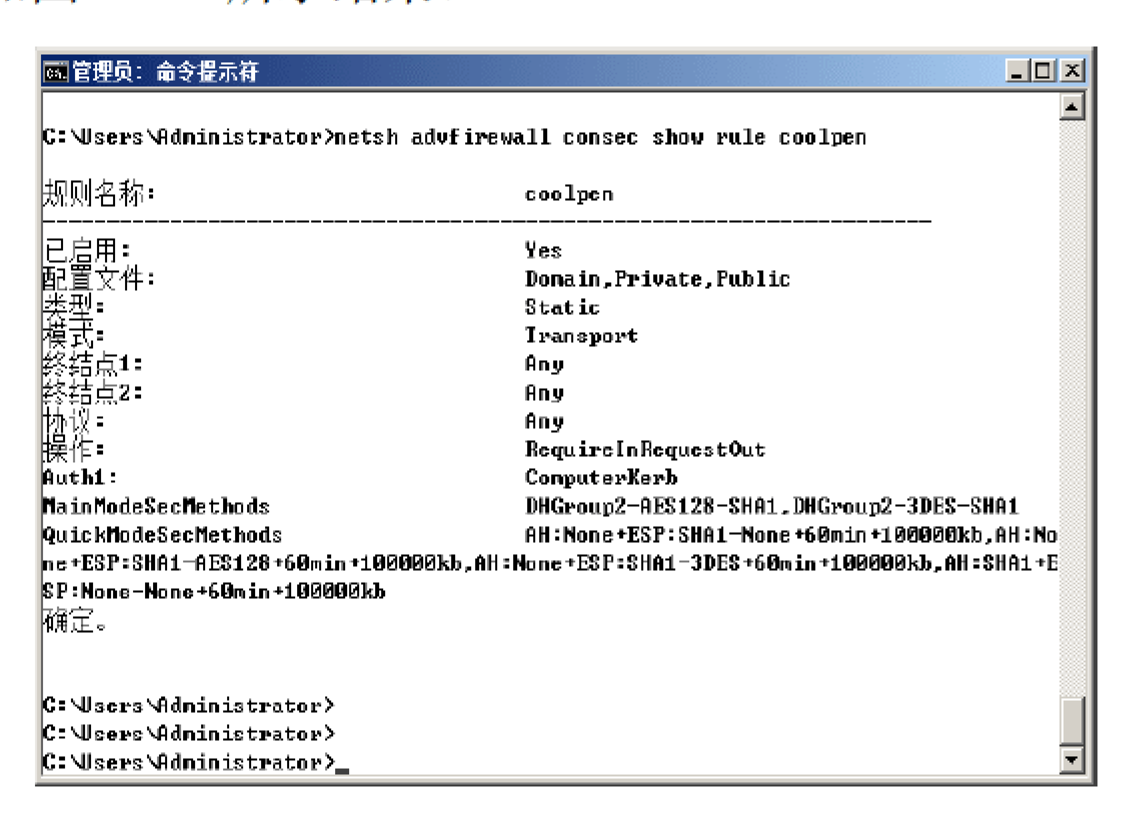


图 15.41　查看规则详细信息

2. 创建子网到子网的安全连接规则

创建从子网 A（192.168.0.0，external ip=60.9.255.48）到子网 B（211.82.218.0，external ip=121.17.46.88）的隧道模式规则，名称为 HSNC，规则类型为“隧道”，身份验证方式为“入站和出站连接请求身份验证”。在命令提示符窗口中输入如下命令：

```
netsh advfirewall consec add rule name="hsnc" mode=tunnel endpoint1=192.168.0.0/16
endpoint2=211.82.218.0/24remotetunnelendpoint=121.17.46.88localtunnelendpoint=60.9.
255.48 action=requireinrequireout
```

回车执行，显示如图 15.42 所示结果，即创建成功。

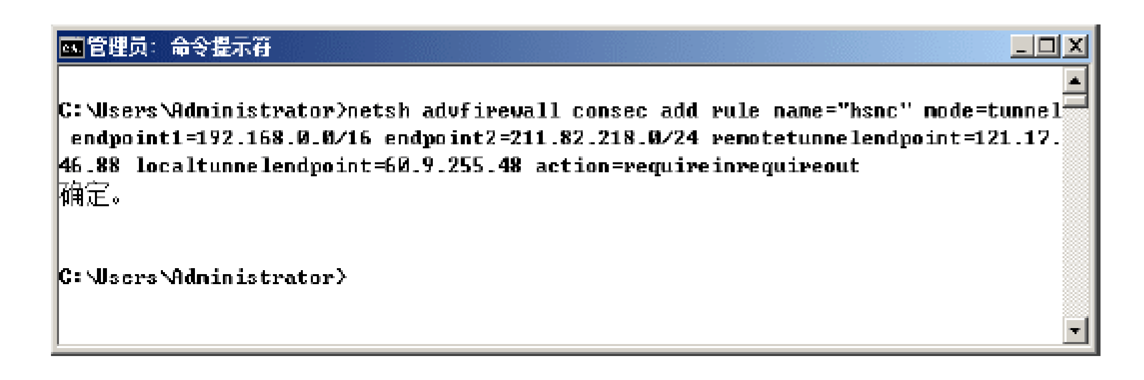


图 15.42　创建子网到子网的安全连接规则

3. 创建访问规则

新增一条允许 messenger.exe 访问入站的规则，名称为“all messenger”，可以在命令提示符窗口中，输入如下命令：

```
netsh advfirewall firewall add rule name="allow messenger" dir=in
program="c:\programfiles\messenger\msmsgs.exe” action=allow
```

回车执行，显示如图 15.43 所示结果。

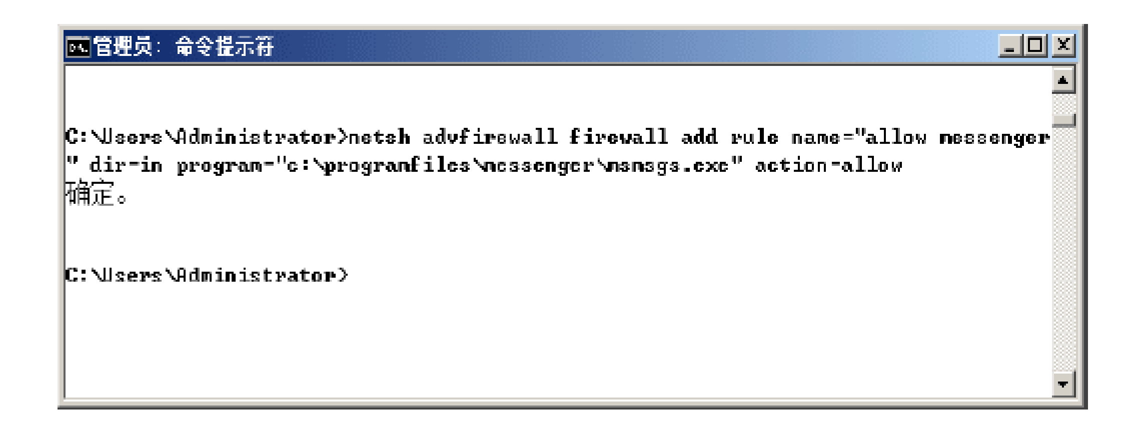


图 15.43　创建入站规则

继续输入如下命令：

```
netsh advfirewall firewall show rule "allow messenger"
```

回车执行，即可查看已经成功创建的如站规则的详细信息，如图 15.44 所示。

```
管理员：命令提示符
C:\Users\Administrator>netsh advfirewall firewall show rule "allow messenger"

规则名称:                             allow messenger
----------------------------------------------------------------------
已启用:                               Yes
方向:                                 In
配置文件:                             Domain,Private,Public
分组:
本地 IP:                              Any
远程 IP:                              Any
协议:                                 Any
边缘遍历:                        No
操作:                                 Allow

规则名称:                             allow messenger
----------------------------------------------------------------------
已启用:                               Yes
方向:                                 In
配置文件:                             Domain,Private,Public
分组:
本地 IP:                              Any
远程 IP:                              Any
协议:                                 Any
边缘遍历:                        No
操作:                                 Allow
确定。

C:\Users\Administrator>_
```

图 15.44　查看入站规则详细信息

15.4.3　netsh firewall>命令环境

netsh firewall>命令环境主要用于管理和配置普通 Windows 防火墙，区别于 Windows Server 2008 中的高级安全 Windows 防火墙，但是在 Windows Server 2008 和 Windows Vista 系统中仍然可用，用法与 nesh advfirewall>类似。

1. 快速查看 Windows 防火墙配置状态

在“netsh firewall”提示符下，输入字符串命令“show state”，单击回车键后，显示如图 15.45 所示“管理员：命令提示符 - netsh”窗口，可以查看系统自带防火墙各个方面的安全配置状态信息。



```
管理员: 命令提示符 - netsh
Microsoft Windows [版本 6.0.6001]
版权所有 (C) 2006 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>netsh
netsh>firewall
netsh firewall>show state

防火墙状态:
-------------------------------------------------------------------
配置文件                          = 标准
操作模式                          = 启用
例外模式                          = 启用
多播/广播响应模式                 = 启用
通知模式                          = 禁用
组策略版本                        = Windows 防火墙
远程管理模式                      = 禁用

所有网络接口上的端口当前均为打开状态:
端口   协议   版本   程序
-------------------------------------------------------------------
当前没有在所有网络接口上打开的端口。

netsh firewall>
```

图 15.45　“管理员：命令提示符 - netsh”窗口

在这里发现了 Windows 系统自带防火墙使用了标准配置文件，启用了例外模式，多播/广播响应模式，禁止了通知模式，所有网络连接接口上没有网络端口被打开。

2. 用命令配置 Windows Server 2008 文件和打印共享

在访问 Windows Server 2008 系统中的网络打印机时，会经常遇到无法访问网络打印机的故障现象，这种故障现象往往都是由于对应系统自带的防火墙禁止文件和打印共享操作连接网络造成的，这时就需要对 Windows Server 2008 系统防火墙进行合适配置，让其允许文件和打印共享操作连接网络。

以管理员身份打开命令提示符窗口，进入 netsh firewall>命令环境。输入如下命令：

```
set opmode enable
```

回车执行，进入系统防火墙的全局操作模式。文件和打印共享操作需要开启 TCP139、TCP445、UDP137、UDP138 端口，管理员可以继续在当前环境下依次输入并执行如下命令：

```
add portopening TCP 139 blah enable subnet
add portopening TCP 445 blah enable subnet
add portopening UDP 137 blah enable subnet
add portopening UDP 138 blah enable subnet
```

成功完成后，显示如图 15.46 所示结果。这时 Windows Server 2008 系统防火墙就会自动开启 TCP139、TCP445、UDP137、UDP138 等端口，一旦端口被成功启用后，就可以通过这些端口访问到安装在 Windows Server 2008 系统中的网络打印机。

```
管理员: 命令提示符 - netsh
Microsoft Windows [版本 6.0.6001]
版权所有 (C) 2006 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>netsh
netsh>firewall
netsh firewall>set opmode enable
确定。

netsh firewall>add portopening TCP 139 blah enable subnet
确定。

netsh firewall>add portopening TCP 445 blah enable subnet
确定。

netsh firewall>add portopening UDP 137 blah enable subnet
确定。

netsh firewall>add portopening UDP 138 blah enable subnet
确定。

netsh firewall>
```

图 15.46　netsh firewall 命令

15.5 Windows 防火墙事件审核配置

Windows 防火墙日志可以记录 Windows 防火墙工作过程中的状态变化，以及防火墙规则的应用情况。通过对 Windows 防火墙产生的事件进行审核，可以帮助用户快速了解网络策略的运行及更改情况，在排除 Windows 防火墙故障时尤为有用。通常情况下，管理员可以通过事件查看器中的相关日志，详细了解工作过程中的状态变化。

15.5.1 启用审核设置

若要配置 Windows 防火墙事件审核，必须以具有系统管理员权限的用户帐户登录系统，启用本地策略中的“审核策略更改”、“审核进程跟踪”和“审核系统事件”策略。单击“开始”按钮，在“开始搜索”文本框中输入“gpedit.msc”，按 Enter 键显示如图 15.47 所示“本地组策略编辑器”窗口。如果是域环境中部署所有客户端 Windows 防火墙，直接以域管理员帐户编辑域策略中的相关设置即可。

图 15.47 “本地组策略编辑器”窗口

1. 审核策略更改

在“本地组策略编辑器”窗口中，双击“审核策略更改”策略，显示如图 15.48 所示“审核策略更改 属性”对话框。选中“成功”或者“失败”复选框，单击“确定”按钮，即可完成策略的设置。

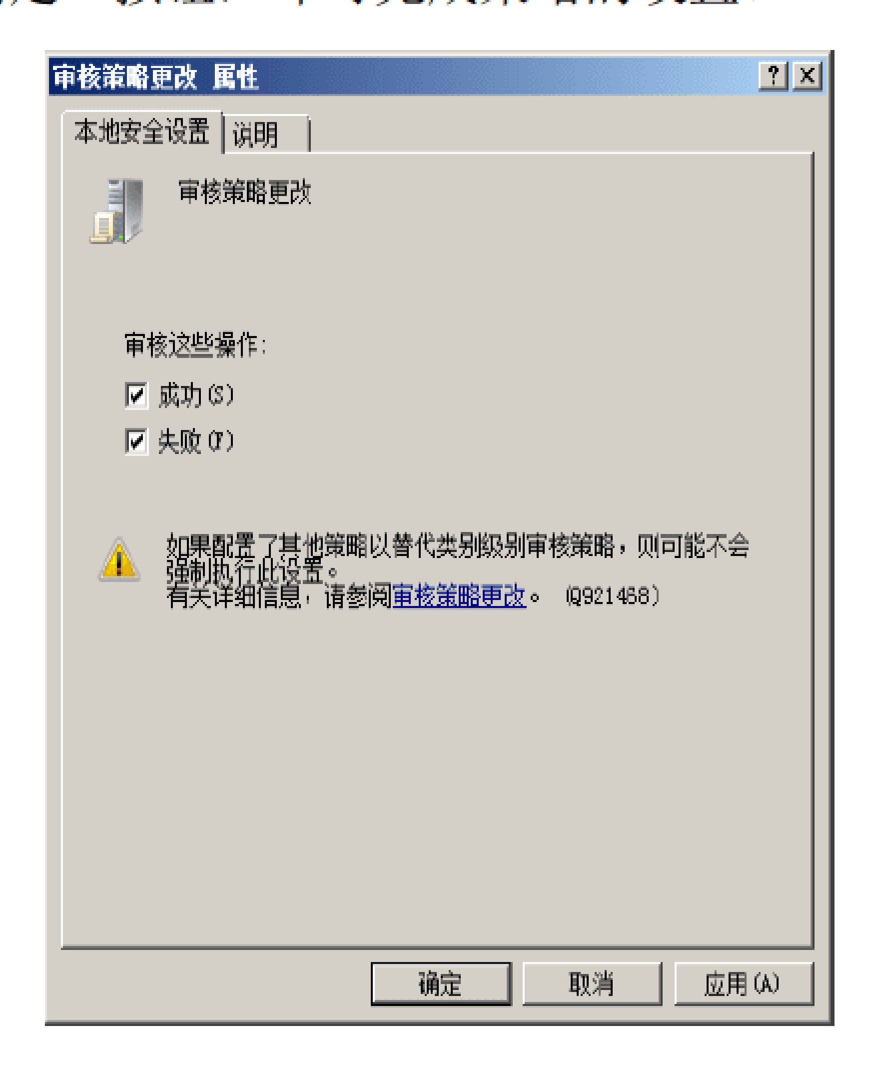


图 15.48 “审核策略更改 属性”对话框



审核策略更改产生的安全事件中，与 Windows 防火墙相关的事件如表 15.3 所示。

表 15.3　与 Windows 防火墙相关的策略更改事件

事件 ID	消息
4944	Windows 防火墙启动时下列策略处于活动
4945	Windows 防火墙启动时被列出规则
4946	Windows 防火墙例外列表已被进行更改，添加规则
4947	Windows 防火墙例外列表已被进行更改，修改规则
4948	Windows 防火墙例外列表已被进行更改，删除规则
4949	Windows 防火墙设置已还原到默认值
4950	Windows 防火墙设置已经更改
4951	规则已忽略因为通过 Windows 防火墙无法识别其主版本号
4952	由于通过 Windows 防火墙无法识别其次要版本号部分规则已被忽略，将强制规则的其他部分
4953	因为无法解析规则，已忽略通过 Windows 防火墙
4954	Windows 防火墙组策略设置已更改，已应用新设置
4956	Windows 防火墙已更改活动配置文件
4957	Windows 防火墙未应用以下规则
4958	由于规则引用此计算机上没有配置项目没有 Windows 防火墙采用以下规则

2. 审核进程跟踪

在“本地组策略编辑器”窗口中，双击“审核过程跟踪”策略，显示如图 15.49 所示“审核进程跟踪 属性”对话框。根据需要选中“成功”或者“失败”复选框，单击“确定”按钮，即可完成策略的设置。

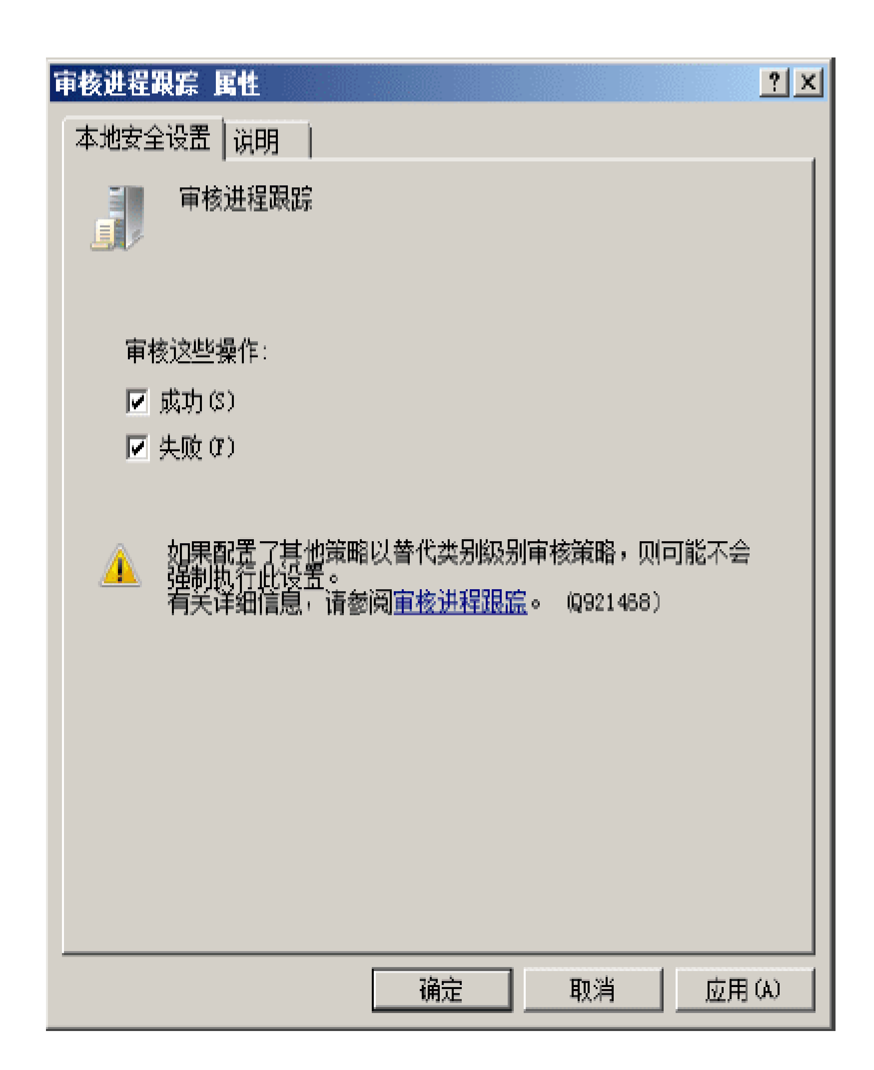


图 15.49　“审核进程跟踪 属性”对话框

由“审核详细跟踪”安全策略设置所生成的安全事件如表 15.4 所示。

表 15.4 审核进程跟踪事件

事件 ID	消息
4688	已创建一个新进程
4689	进程已退出
4692	尝试数据保护主密钥备份
4693	尝试对数据保护主密钥恢复
4694	尝试保护的审计保护数据
4695	尝试未保护的审计保护数据
4696	主令牌被分配给处理
5712	试图远程过程调用（RPC）

3. 审核系统事件

审核系统事件中包括 Windows 防火墙应用程序的工作过程，如启动、停止等。在“本地组策略编辑器”窗口中，双击“审核系统事件”策略，显示如图 15.50 所示“审核系统事件 属性”对话框。根据需要选中“成功”或者“失败”复选框，单击“确定”按钮，即可完成策略的设置。

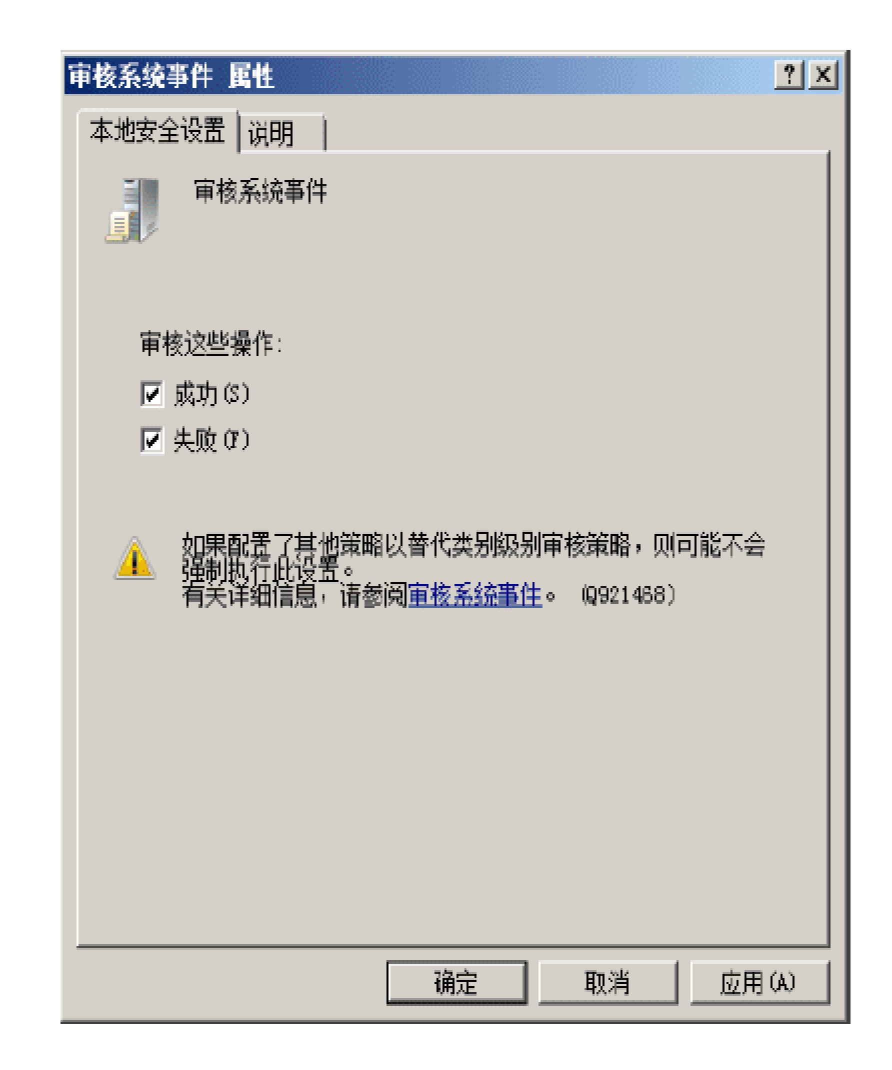


图 15.50 “审核系统事件 属性”对话框

审核策略更改产生的安全事件中，与 Windows 防火墙相关的事件如表 15.5 所示。

表 15.5 与 Windows 防火墙相关的系统事件

事件 ID	消息
5024	Windows 防火墙服务成功启动
5025	Windows 防火墙服务已停止
5027	Windows 防火墙服务无法从本地存储器检索安全策略。服务将继续强制当前策略
5028	Windows 防火墙服务无法分析新安全策略。服务将继续与当前实施策略
5029	Windows 防火墙服务无法初始化驱动程序。服务将继续以强制当前策略
5030	Windows 防火墙服务无法启动



（续表）

事件 ID	消息
5032	Windows 防火墙无法通知用户它阻止应用程序接受传入连接在网络上
5033	Windows 防火墙驱动程序成功启动
5034	Windows 防火墙驱动程序已停止
5035	Windows 防火墙驱动程序无法启动
5037	Windows 防火墙驱动程序检测到关键运行错误。终止

15.5.2 查看审核功能记录

启用审核策略后，即可通过 Windows Server 2008 系统的事件查看器，查看和管理 Windows 防火墙工作过程中产生的安全事件。事件日志中记录了事件发生的时间、事件来源、用户帐户、操作代码及了解详细相关信息的超级链接。在 Windows Server 2008 系统中，事件日志详细信息的基础结构完全符合 XML 架构，而且可以访问代表指定事件的 XML。

01 依次选择“开始”→“管理工具”→“事件查看器”选项，打开“事件查看器”窗口，依次展开“Windows 日志”→“安全”选项，如图 15.51 所示。系统默认已经启动“预览窗格”功能，即在事件列表中选择时间后，将自动显示相应预览信息。

02 单击“事件 ID”标签，按照时间 ID 排序后，找到希望查看的 Windows 防火墙事件即可。双击事件显示如图 15.52 所示“事件属性 － 事件 5024”对话框，在“常规”选项卡中，可以查看该事件的来源、类型、级别、时间等信息。

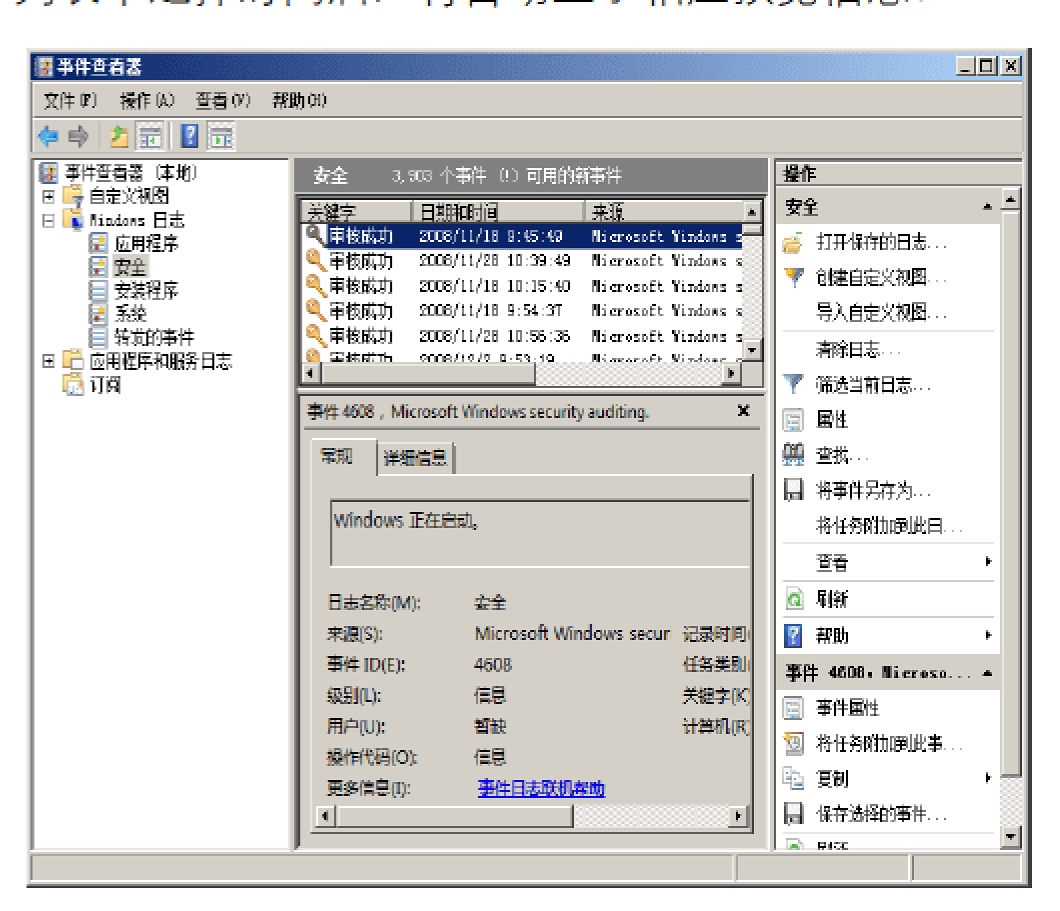


图 15.51 “事件查看器”窗口



图 15.52 “事件属性 – 事件 5024”对话框

03 单击“详细信息”切换至如图 15.53 所示“详细信息”选项卡，系统默认是以“友好视图”方式显示的。

04 选择“XML 视图”单选按钮，即可以 XML 视图方式显示事件详细信息，如图 15.54 所示。

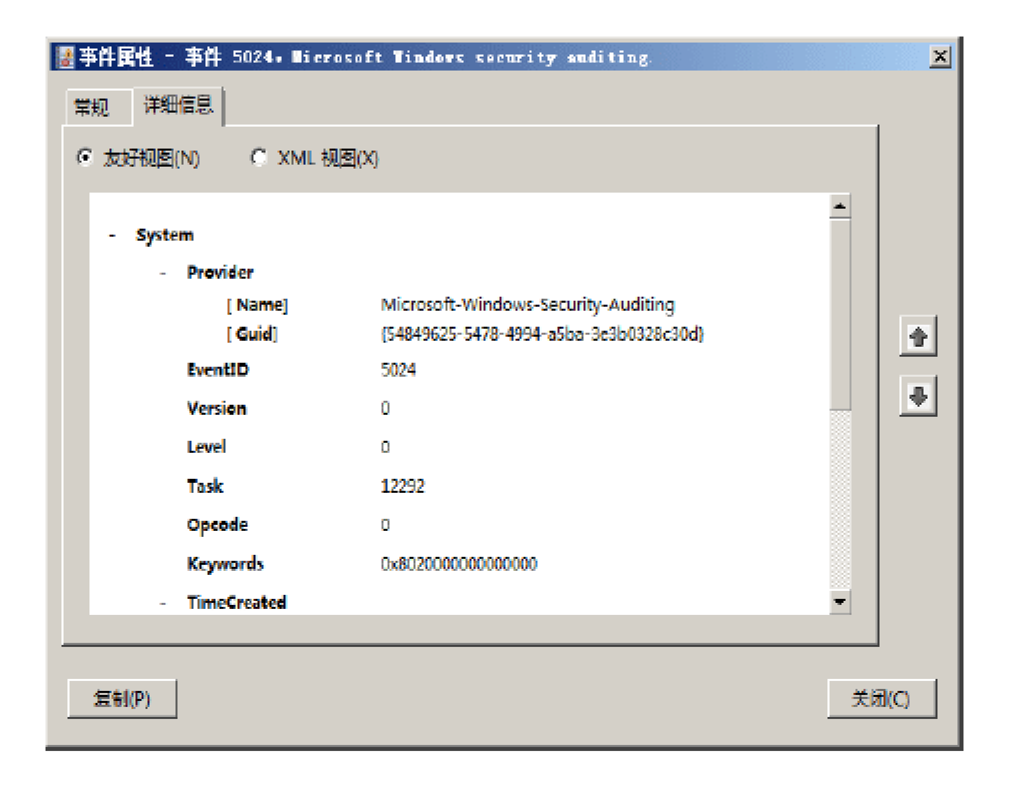
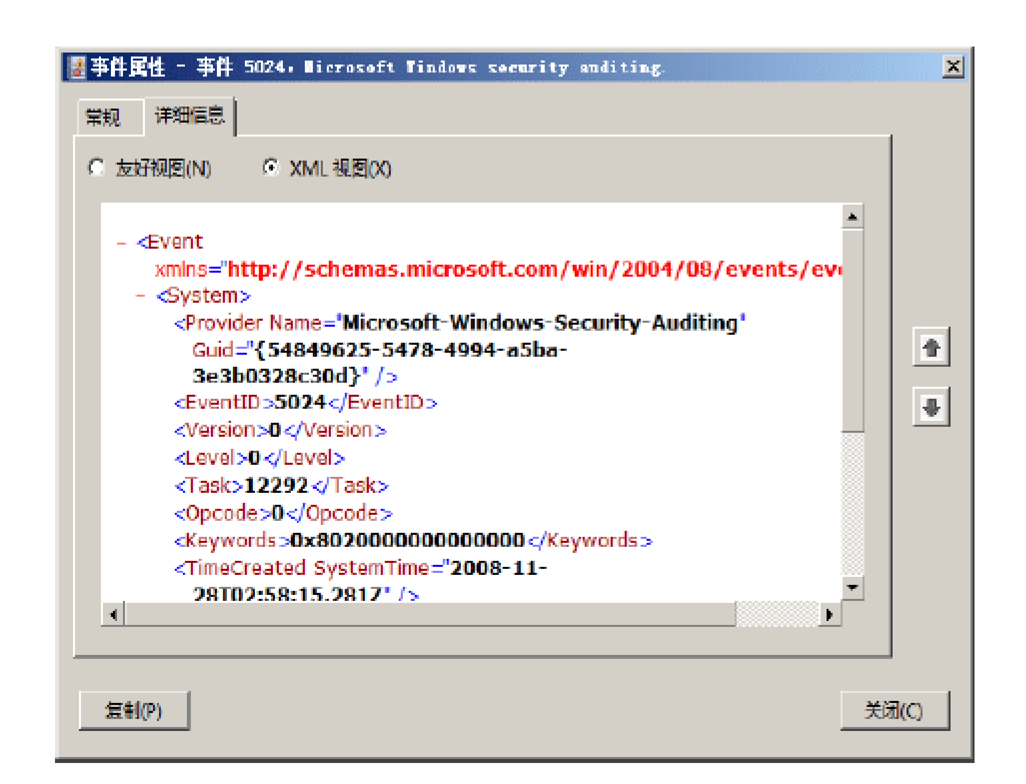


图 15.53　友好视图




```
- <Event
  xmlns="http://schemas.microsoft.com/win/2004/08/events/eve
- <System>
  <Provider Name="Microsoft-Windows-Security-Auditing"
   Guid="{54849625-5478-4994-a5ba-
   3e3b0328c30d}" />
  <EventID>5024</EventID>
  <Version>0</Version>
  <Level>0</Level>
  <Task>12292</Task>
  <Opcode>0</Opcode>
  <Keywords>0x8020000000000000</Keywords>
  <TimeCreated SystemTime="2008-11-
   28T02:58:15.2817" />
```

图 15.54　XML 视图

05 单击“关闭”按钮，关闭“事件属性”对话框即可。

15.5.3　筛选 Windows 防火墙事件

启动任何一项审核策略都会产生大量的事件日志，其中与 Windows 防火墙运行相关的内容并不多。通过筛选相关日志，可以快速查看需要的目标事件。在事件筛选器中，用户可以指定关键字、事件 ID、事件来源等筛选信息。

01 在“事件查看器”窗口中，依次展开“Windows 日志”→“安全”选项。在“操作”栏中单击“筛选当前日志”链接，显示如图 15.55 所示“筛选当前日志”对话框。例如按照事件 ID 筛选，在“包括/排除事件 ID”文本框中，输入希望查看的事件 ID 号或 ID 范围。

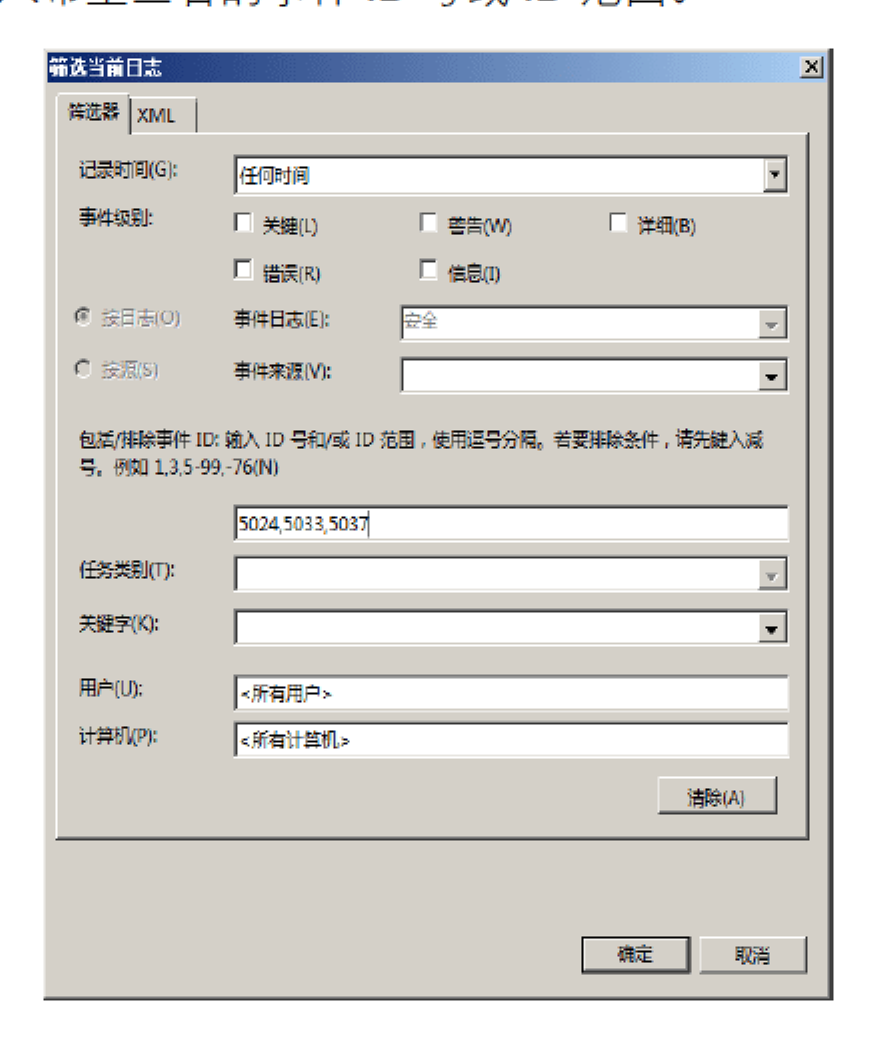


图 15.55　“筛选当前日志”对话框



提示　如果要查看多个事件，则 ID 号之间必须以逗号分隔。如果要包括一个范围的 ID，例如 5024 到 5033（包括 5033），可以输入 5024-5033。如果希望筛选器显示包括除某些 ID 以外所有 ID 的事件，请输入这些排除的 ID，前面加一个减号。例如，若要包括 5024 和 5033 之间除 5032 以外的所有 ID，则可以输入 5024-5033,-5032。



02 单击“确定”按钮，即可开始筛选。完成后，显示如图 15.56 所示结果。直接在“已筛选日志”列表中，双击希望查看的事件日志即可。

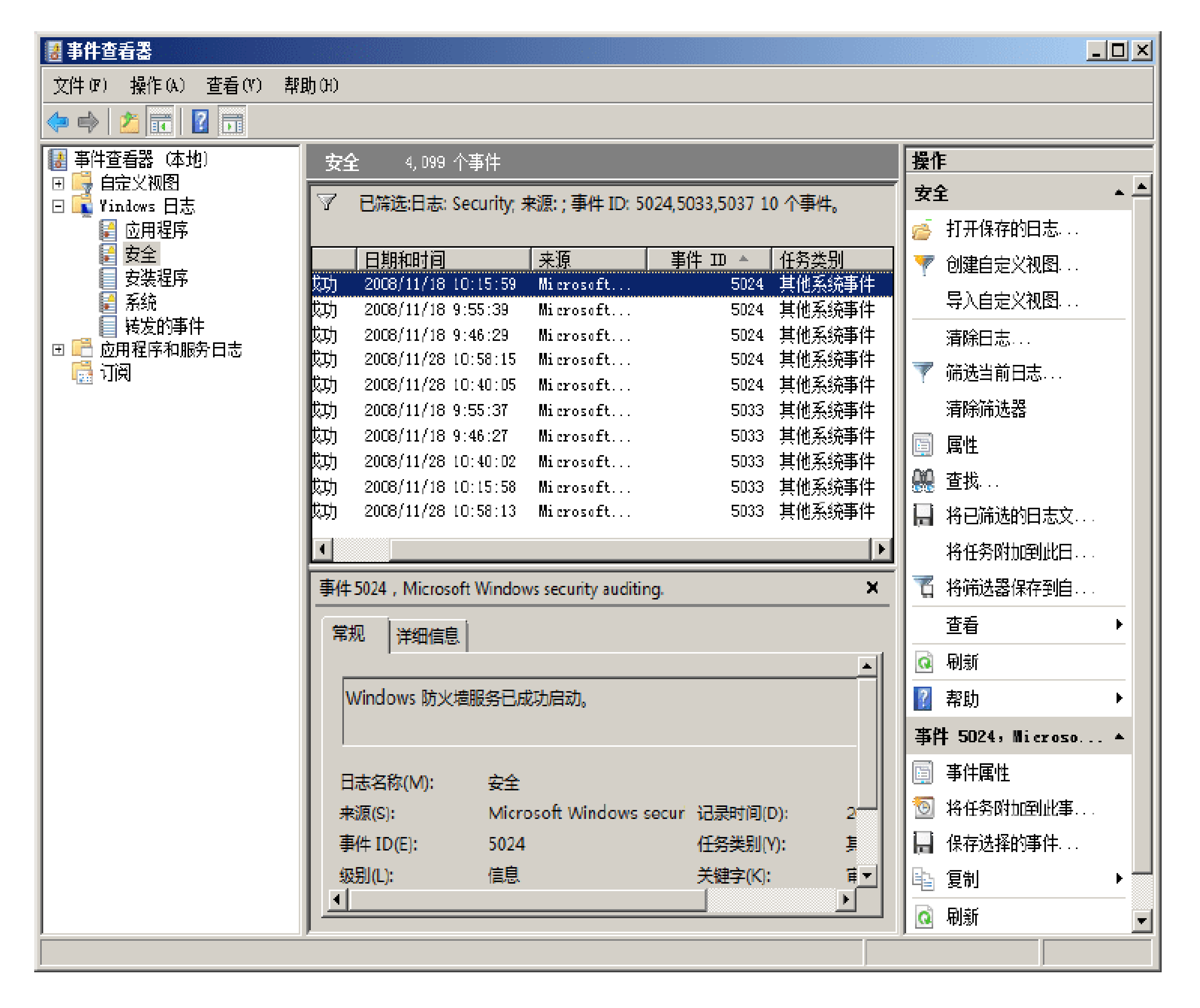


图 15.56　筛选事件日志

03 单击“清除筛选器”链接，即可清除当前筛选结果，返回相应的事件分组。

15.5.4　配置 Windows 防火墙日志文件

Windows 防火墙应用程序本身在运行过程中，也会产生相应的日志，与系统事件不同的是，这些日志主要记录运行过程中，各个防火墙规则的变化情况，并且用户可以为不同作用域的防火墙规则，指定不同的日志文件。需要注意的是，该日志默认是未配置的，即不对任何规则执行情况进行记录。

01 打开“高级安全 Windows 防火墙”窗口，右击“本地计算机 上的高级安全 Windows 防火墙 属性”，显示如图 15.57 所示“本地计算机 上的高级安全 Windows 防火墙 属性”对话框。

02 在“日志”选项区域中单击“自定义”按钮，显示如图 15.58 所示“自定义 专用配置文件 的日志设置”对话框。在“名称”文本框中，显示的是日志文件的默认保存路径和名称：%Systemroot%\System32\LogFiles\Firewall\pfirewall.log。在“大小限制”文本框中，可以自定义日志文件的最大值，以确保不丢失任何信息。在“记录丢弃的数据包”和“记录成功的连接”下拉列表中，均选择“是”选项即可，系统默认选择“否”选项，即不启用日志。

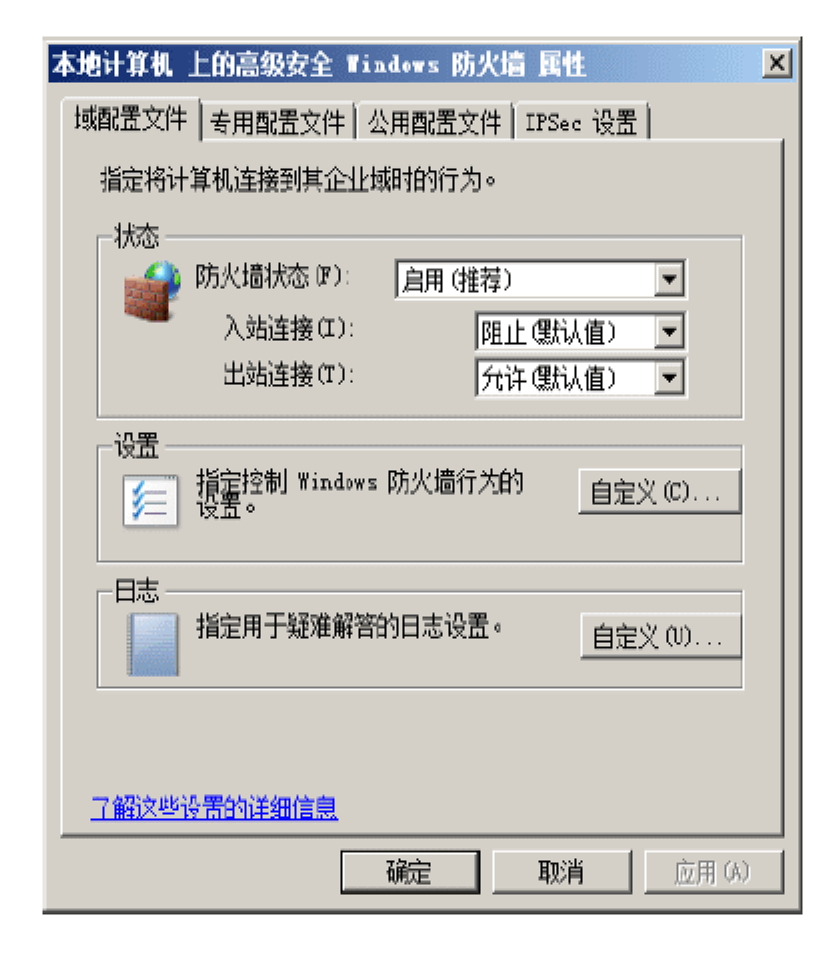


图 15.57 “本地计算机 上的高级安全 Windows 防火墙 属性”对话框

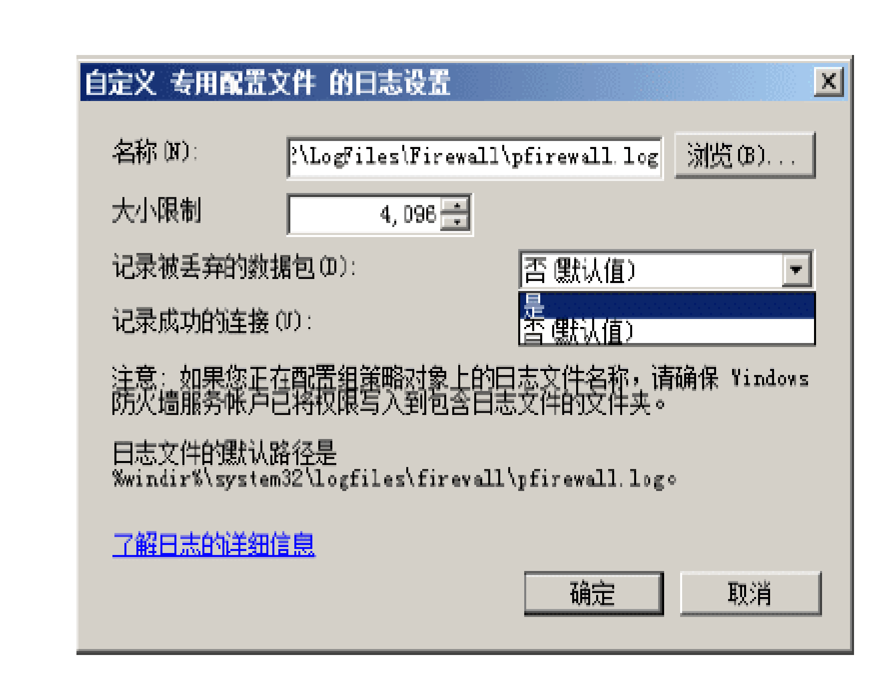


图 15.58 “自定义 专用配置文件 的日志设置”对话框

03 单击“确定”按钮，保存设置即可。

在“专用配置文件”和“公用配置文件”选项卡中，同样可以相应作用域的防火墙规则配置日志文件。既可以使用和“域配置文件”相同的目标日志文件，也可以重新指定。为了便于查看和管理，建议为不同作用范围的防火墙规则，指定不同的日志文件。

小　　结

高级安全 Windows 防火墙是 Windows Server 2008 和 Windows Vista 系统的一个亮点，本章主要介绍了基本 Windows 防火墙和高级安全 Windows 防火墙的配置和应用，包括开启或关闭防火墙、设置例外程序、发布应用服务等。在域环境中，客户端防火墙的配置不当，往往会影响彼此之间的通信，使用组策略统一配置客户端防火墙，无疑是最好的选择。高级安全 Windows 防火墙集中了大部分的安全配置功能，并且可以对所有出站和入站请求进行双向验证。Windows Server 2003 系统中的防火墙日志和 ICMP 协议设置，已经被转移到高级安全 Windows 防火墙中。除此之外，管理员可以通过创建 IPSec 连接安全规则，灵活控制端到端的连接安全。为了便于管理员掌握防火墙规则的应用情况，建议启用并配置防火墙事件审核策略，生成的系统事件，可以在 Windows 事件查看器中查看。

习　　题

1. 如何使用 netsh advfirewall 工具配置 Windows 防火墙？
2. 如何添加组策略编辑器？
3. 使用 IPSec，如何确保网络安全？
4. 怎样启用配置审核功能？



实验：阻止用户登录 MSN

实验目的

运用组策略部署客户端 Windows 防火墙，可以根据需要灵活创建防火墙规则。

实验内容

以域管理员帐户登录到域控制器，为所有客户端创建组策略，编辑高级安全防火墙的入站规则，禁止 MSN 应用程序访问 Internet，MSN 使用的默认端口是 1863。

实验步骤

1. 以域管理员帐户登录到域控制器，将所有客户端计算机移动到新创建的组织单位中。
2. 创建基于新建组织单位的组策略。
3. 打开组策略管理编辑器窗口。
4. 创建入站规则，规则内容为禁止所有客户端计算机的 UDP 1863 端口访问 Internet。
5. 在客户端计算机上重新登录到域，刷新组策略，验证防火墙规则是否生效。

第16章

Windows 网络访问保护

远程访问是大多数局域网中比较常用的功能之一，由于不安全客户端远程拨入导致的网络瘫痪故障也时有发生。Windows Server 2008 系统的网络访问保护功能，可以通过网络策略服务器对客户端拨入请求进行身份验证和健康状态评估，只有达到网络健康标准的客户端，才允许接入内部网络，未达到网络标准的客户端，可以通过指定的修正服务器修复计算机的状态后才允许接入内部网络。

本章导读

- NAP 简介
- NPS 的安装
- 配置 IPSec 强制
- 配置 DHCP 强制
- 配置 VPN 强制



16.1　NAP 简介

网络访问保护（Network Access Protection，简称 NAP）是 Windows Server 2008 操作系统中内置的策略执行平台。为了更好地保护网络安全，NAP 强制计算机符合系统健康要求，对不符合策略要求的用户进行隔离并对其进行帮助提示，直至符合要求才能正常访问网络。

16.1.1　NAP 组件

启用 NAP 网络基础结构的组件主要包括以下几部分:

- NAP 客户端。支持 NAP 的计算机有 Windows XP SP3、Windows Vista、Windows Server 2008 操作系统的计算机;
- NAP 强制点。NAP 强制点是指使用 NAP 的服务器和网络设备，使网络策略服务器（Network Policy Server，简称 NPS）作为 NAP 的健康策略服务器来评估客户端的健康状态,从而判断网络访问或通信是否被允许,以及不符合的客户端执行相应的修正动作;
- NAP 健康策略服务器。NAP 健康策略服务器是指在 Windows Server 2008 的计算机，以及存储健康要求策略和提供健康状态验证的 NPS 服务。NPS 代替了 Internet 身份验证服务、RADIUS 服务器和 Windows Server 2003 提供的代理。NPS 也可以作为网络访问的身份验证、授权和记账（AAA）服务器。当作为 AAA 服务器或 NAP 健康策略服务器时，NPS 通常为网络访问和健康要求策略的集中配置使用单独的服务器。NPS 访问也可以运行在基于 Windows Server 2008 的 NAP 强制点上，例如 DHCP 服务器。但是在这些配置中，NPS 服务是作为 RADIUS 代理与 NAP 健康策略服务器交换 RADIUS 消息的;
- 健康要求服务器。为 NAP 健康策略服务器提供当前系统健康状态的计算机;
- 活动目录域服务。存储帐户证书和组策略设置的 Windows 目录服务。虽然不需要健康状态验证，但活动目录需要 IPsec 保护通信，802.1X 验证连接，以及远程访问 VPN 连接;
- 受限网络。将不满足健康要求策略的计算机放置在首先的网络中，并通过网络中的修正服务器，修正不符合健康策略要求的方面使其成为符合要求的健康客户端;
- 不支持 NAP 的计算机。不支持 NAP 的计算机将会被放置在受限的网络中。

16.1.2　NAP 系统工作机制

网络访问保护主要分为 4 个部分：策略验证、隔离、补救和持续监控。

1. 策略验证

策略验证是指 NAP 根据网络管理员定义的一系列规则，对客户端计算机系统状态进行评估。NAP 在计算机尝试连接到网络时会使用安全监控程序和定义的策略相比较，符合这些策略的计算机视为良好的计算机，而不符合其中一项或多项标准的计算机则被认为是状态不良的计算机。通过这些策略可以检查客户端计算机是否有防病毒软件，是否开启防火墙，是否缺少某个安全补丁等。

2. 隔离

如果没有通过验证策略，则视为网络限制，即隔离。根据网络管理员定义的策略，NAP 可以将计算机的网络连接设置为各种状态，例如一台计算机因没开启防火墙而视为状态不良，NAP 可以将该计算机置于隔离网络中，使其与网络中其他计算机隔绝，直至恢复健康（开启防火墙）为止。

NAP 有两种部署模式，即监控模式和隔离模式。在监控模式下，即使发现授权用户计算机不符合策略，也可以访问网络，但该状况会被记入日志，管理员可以指导用户如何让计算机符合策略。在隔离模式下，不符合策略的计算机只能有限访问网络，它们可以在该网络上找到符合策略的资源。

3. 补救

对于被隔离的计算机，NAP 提供了补救策略，即被隔离的计算机无需网络管理员干预即可修复影响运行状态的问题。受限网络允许状态不良的计算机访问特定的网络资源，例如 Windows Server Update Services 服务器。在没有恢复健康之前，不能访问网络中的其他计算机。

4. 持续监控

强制计算机在与网络保持连接期间，始终监控这些可保持状态良好的策略。如果计算机状态与策略不符，例如禁用了 Windows Update，则 NAP 将自动开启自动更新，直至恢复正常状态后，才可以访问网络。

16.1.3 强制方式

Windows XP SP3、Windows Vista 和 Windows Server 2008 中的 NAP 支持 4 种类型的网络访问和通信：

- IPsec 保护通讯；
- 远程访问 VPN 连接；
- IEEE8.2.1x 身份验证的网络连接；
- DHCP 地址配置。

管理员可以使用这些类型的网络访问或通信（也叫做 NAP 强制方式）来独立或共同限制不符合计算机的访问或通信。



1. IPsec 强制

IPsec 强制由健康证书服务器和 IPsecNAPEC 组成，当确定客户端复合时，健康证书服务器颁发 X.509 证书隔离它们。当 NAP 客户端与 Intranet 上的其他 NAP 客户端通信时，使用这些证书对 NAP 客户端进行身份验证。

IPsec 强制将网络上的通信限制为被认为是符合的那些节点，原因是用户想利用 IPsec，为受保护的通信在每个 IP 或每个 TCP/UDP 端口号上指定要求。成功连接并且获得有效的 IP 地址配置之后为符合的计算机限制通信。IPsec 强制是 NAP 中限制网络访问的最强形式之一。

2. 802.1X 强制

802.1.X 强制由 NPS 服务器和 EAPHOSTNAPEC 组件组成。使用 802.1X 强制，NPS 服务器知道 802.1 访问点（以太网交换机或无线访问点）在 802.1X 客户端上放置受限制的访问配置文件，直到它执行一组修正功能为止。受限制的访问配置文件可以由一组 IP 数据包筛选器或虚拟 LAN(VLAN)标识符组成，用于限制 802.1X 客户端的通信。802.1X 强制为通过 802.1X 连接访问网络的所有计算机的网络访问提供比较强的限制。

3. VPN 强制

VPN 强制组件包括 Windows Server 2008 中的 NPS 和 Windows XP SP3、Windows Vista 和 Windows Server 2008 远程访问客户端上的 VPN 强制客户端。

使用 VPN 强制，VPN 服务器可以在计算机尝试对网络进行 VPN 连接时强制健康策略要求。VPN 强制通过 VPN 连接访问网络的所有计算机的网络访问提供比较强的限制。VPN 强制为所有通过远程访问 VPN 连接访问网络的计算机，提供了有效的受限网络访问。

4. DHCP 强制

DHCP 强制组件包括 Windows Server 2008 DHCP 服务器中的 DHCP ES 和 Windows XP SP3、Windows Vista 和 Windows Server 2008 DHCP 客户端中的 DHCP EC。

使用 DHCP 强制，DHCP 服务器可以在计算机尝试租用或续订网络上的 IP 地址配置时强制健康策略要求。DHCP 强制是最简单的部署强制，因为所有 DHCP 客户端计算机必须租用 IP 地址，管理员可以任意修改，所以 DHCP 强制是 NAP 中受限网络访问中最弱的形式。

注意



NAP 的作用只是用来检查将要连接网络的计算机是否具备完备的安全补丁，是否有安全配置方面的错误等，以此提升计算机网络的安全性，不能取代系统内的安全软件。

16.1.4　NAP 的应用环境

网络内部安全已经成为网络安全的重点，用户水平参差不齐，使用习惯各不相同。例如，如果网络中没有安装软件更新或者防病毒软件的客户端，很可能导致整个网络遭受攻击。NAP 可以很好地解决这一难题，通常情况下，它可以应用于如下保护环境。

1. 保护漫游计算机的健康

网络中应用笔记本移动办公的用户越来越多，例如需要经常携带笔记本出差的用户，笔记本需要经常连接不安全的外部网络，没有安装更新补丁，没有更新病毒库，或者已经感染病毒，一旦连接到公司网络，需要进行安全检查。

2. 保护桌面计算机的健康

网络中相对比较固定的工作站，虽然受到网络防火墙的保护和安全策略限制，但是由于经常接入 Internet、连接移动设备、收发电子邮件等，也可能存在一定的安全隐患，有必要接受补丁包获得更新，更新病毒库。

3. 保护来访用户计算机的健康

有时候来访用户的计算机需要连接到内部网络，但是很难保证这些计算机符合网络内部的安全策略，如果强行接入网络，可能会有安全威胁。此时，可以通过网络访问保护功能在技术层面进行访问限制。当客户计算机连入内部网络之后，NAP 可以将客户计算机重定向到一个隔离的网段、会自动连接到修正服务器，对客户计算机实施制定的安全策略，例如进行自动更新、修复漏洞等，在修复安全之后，客户计算机可以自动连接到内部网络，以上操作自动完成，不耽误业务的进展。

4. 保护家庭计算机的健康

网络中的用户有时候会将工作带到家中处理，需要通过 VPN 等方式将家中的计算机连接到公司内部网络访问资源，此时家中的计算机有可能对公司内部网络造成安全威胁。使用 NAP 功能可以设置检查家庭计算机，可以将连接入的家庭计算机限制到隔离网段，进行健康修复，直到安全为止。

16.1.5 部署 NAP 的意义

计算机网络安全的防范应该是全方位的，网关、防火墙可以阻止病毒入侵网络，访问权限控制可以阻止用户越权访问，这些都是针对已经发生的网络安全事件而言的。网络访问安全防护则主要用于评估远程用户系统的健康程度，是否符合健康策略要求，是一种防患于未然的防护方式。NAP 系统可以有效防止恶意软件、病毒等在网络中的传播。

1. 恶意软件及其对企业计算机的影响

用户对恶意软件并不陌生，如间谍软件、木马程序、广告软件等。通常情况下，恶意软件并不会直接破坏系统数据或用户信息，而是向其服务器端发送计算机活动报告，以便于恶意用户对计算机的远程控制。Internet 是一个开放性极高的环境，一台安全性不高的计算机可能会在几分钟之内被地址和端口扫描软件入侵。



（1）恶意软件如何进入企业网络

通常企业网络环境都不是直接连接到 Internet 上的，只有部分计算机直接连接到 Internet，为客户或商业伙伴提供 Internet 服务。大部分的计算机和 Internet 之间被防火墙和代理服务器等边界系统隔离。所以企业网络中的计算机通常不会被来自 Internet 的病毒扫描攻击，但是对防火墙或代理服务器提供的边界安全，会面对如下问题：

- 通过在计算机上执行基于特洛伊木马的病毒：企业网络中的用户可能在不经意间就从 E-mail、Web 页面或 Internet 上下载的其他类型的文件中就感染了病毒。其中，E-mail 附件是传播特洛伊木马病毒最常见的方式，Web 页面是另外一种常见的方式；
- 移动和连接其他网络的移动计算机：移动计算机典型代表是便携式计算机，即通常所说的笔记本电脑。用户将便携式计算机带到家里、商业旅途中或其他具有无线热点的公共场所中。每次用户都可以将便携式计算机连接到非企业网络上，此时，便携式计算机都可能受到网络级病毒的攻击；
- 职员远程访问：当职员使用远程访问连接企业网络时，理论上如同在职员所在地到企业网络端口之间有以太网线路一样。通过逻辑连接，企业网络可能会受到网络级病毒的攻击；
- 来宾计算机：当企业的来宾（如顾问、提供商或商业伙伴）使用计算机连接企业网络时，他们所使用的计算机之前可能已经受到网络级病毒的攻击。

（2）恶意软件的影响

对于 Internet 和专有网络来说，恶意软件可能会带来直接的经济影响，例如，机密信息的泄露、知识产权的丢失、带宽的浪费、计算机行为的不可用，以及为了从所有感染的计算机上移除恶意软件所花费的时间等。

2. 恶意软件防护技术

为了防止恶意软件的传播，IT 企业开始防止未来病毒的感染。从而出现了一系列的恶意软件防护技术以及从事该工作的很多企业和用户。恶意软件防护程序是用来防止恶意软件安装和传播的。恶意软件防护程序具有如下形式：

- 杀毒软件：在文件复制或下载时监视已知的恶意软件。杀毒软件通常使用本地病毒库来识别 E-mail 和文件中的恶意软件。如果恶意软件被检测到，杀毒软件将会移除恶意软件或者阻止文件被存储或执行。因为会不停的有新型的病毒被创建，所以杀毒软件的病毒库需要定期更新；
- 垃圾邮件过滤：用来阻止不需要的 E-mail 消息存储到 E-mail 邮箱的软件。垃圾邮件是一种传播病毒或间谍软件常用的方式；
- 反间谍软件：从计算机上检测和移除已知间谍软件和广告软件的软件。如同杀毒软件一样，反间谍软件必须定期更新，使其可以阻止最新的间谍软件的安装。例如，Windows Vista 中的 Windows defender 就是一款反间谍软件。

除了恶意软件防护软件之外，下列技术也可以防止恶意软件：

- Windows 计算机的自动更新：对于运行 Windows 的计算机，一些类型的病毒会针对系

统安全隐患进行攻击，所以安全更新是很有必要的。病毒会尝试攻击没有进行更新的计算机。为了在病毒编写者写出恶意软件并传播之前进行自动安全更新，微软会在发现漏洞的第一时间开发并发布补丁程序，供用户下载和安装。根据用户制定的计划，运行 Windows Vista、Windows Server 2008、Windows XP 或 Windows Server 2003 的计算机，可以获取 Windows 更新 Web 页面和下载最新的安全更新，并自动进行安装。Windows 更新降低了 IT 管理者为了保持计算机更新始终最新的负担；

- 基于主机的全状态防火墙：基于主机的全状态防火墙运行在计算机上，监视网络通信的数据包，阻止计算机发送或接收恶意通信。一些病毒会通过扫描本地子网可用计算机来尝试自动复制，然后攻击找到的计算机。如果成功，那么病毒将会从一台计算机复制到另外一台。如果一台受感染的计算机迁移，那么病毒就开始攻击新的子网中的计算机。例如，当便携式计算机在家庭网络受到感染，病毒将会被携带到企业的专有网络。基于主机的全状态防火墙，如 Windows Vista、Windows Server 2008、Windows XP SP2 和 Windows Server 2003 SP1 或 SP2，将会丢弃所有不符合计算机请求回复的入站通信，或被允许的主动提供的通信。例如，符合用户或计算机的 Web 页面请求的通信就是请求入站通信。由于计算机运行服务器服务而被允许，并且必须接收主动提供的请求，就是例外通信的例子。因为通常的基于网络的病毒依靠主动提供的入站通信来进行传播和攻击计算机，启用连接到 Internet 和内网的计算机上的基于主机的全状态防火墙，可以阻止这种类型病毒的传播。

为了防止恶意软件进入和蔓延在企业网络中，管理员需要确保如下工作：

- 确保用户主机计算机正在使用当前权限级别的网络服务和用户帐户。通过降低用户的权限级别，可以有效的阻止恶意软件安装在主机计算机上。例如，运行 Windows Vista 的计算机使用用户帐户控制（UAC）来降低被攻击的危险性；
- 使用恶意软件防护软件，定期进行更新；
- 启用自动更新，当 Windows 升级包可用时立即安装。企业网络也可以通过中央服务器（如 Windows 服务器更新服务）来配置更新服务；
- 使用基于主机的全状态防火墙，如 Windows 防火墙，来阻止网络级病毒的入侵。

3. 计算机系统健康和监视

恶意软件防护技术的使用为 IT 管理员带来了新的问题，即确定和监视内网中的计算机系统健康。该系统健康由计算机当前的配置状态定义，包括一系列的恶意软件防护技术、及其当前状态和其他配置设置。

（1）确定系统健康要求

系统健康的定义会根据企业安装的恶意软件防护技术、计算机配置和其他安全需求而改变。为了设置系统健康需要的参数，管理员需要注意如下问题：

- 杀毒软件
  - 在整个企业网络的所有计算机上均安装防毒程序；
  - 当前计算机的防毒签名文件或其他更新需要考虑健康问题。
- 垃圾邮件过滤软件
  - 在整个企业网络中安装垃圾邮件过滤软件；
  - 当前计算机的垃圾邮件过滤更新需要考虑健康问题。



- 反间谍软件
  - 反间谍软件遍及整个企业网络；
  - 当前计算机的反间谍更新需要考虑健康问题。
- 操作系统自动更新
  - 在整个企业网络启动 Windows 自动更新；
  - 对于考虑健康状况的计算机启用自动更新；
  - 当前计算机安装的更新需要考虑健康问题。
- 基于主机的全状态防火墙
  - 在整个企业网络启用基于主机的全状态防火墙；
  - 对于考虑健康状况的计算机必须启用防火墙的问题。对于考虑健康状况的计算机需要配置的例外。
- 其他配置设置
  - 根据企业安全策略需要其他配置设置；
  - 对于考虑健康状况的计算机需要的设置。

例如，管理员可以创建系统健康策略，要求所有计算机必须满足如下条件：

- 所有操作系统更新必须在指定日期进行安装；
- 必须安装杀毒软件，并运行其监视入站和出站文件；
- 杀毒软件必须安装最新版本的病毒库；
- 必须安装垃圾邮件过滤软件，并用其监视入站的 E-mail 消息；
- 垃圾邮件过滤软件必须安装最新的更新；
- 安装并启用基于主机的全状态防火墙；
- 基于主机的防火墙必须拥有一个授权的排除列表；
- 计算机上的 TCP/IP 协议栈必须禁用 IP 路由；
- 计算机上的 TCP/IP 协议栈必须启用自动配额制。

需要注意的是，管理员面对的最大问题不是为系统健康设置要求，而是保证企业网络中的所有计算机满足这些要求，以及为不满足要求的计算机执行强制机制。

（2）强制系统健康要求

确定系统健康是否满足企业网络中计算机的强制系统健康要求。换句话说，如果企业网络中的计算机不满足系统健康的要求，就会存在问题。例如可以设置不符合系统健康要求的计算机禁止与网络中的其他计算机进行通信。

尽管大部分的恶意软件防护软件都拥有自己的保持更新的机制，但却没有系统健康要求的强制机制。例如如果杀毒程序没有进行最近的更新，那么对于计算机和计算机用户来说就没有保障。

为了确保系统健康可强制，在局域网中必须拥有一台中央计算机来评价系统健康，而且对其使用企业的系统健康要求进行配置。网络中尝试连接通信的客户端计算机必须拥有自己的健康评估，以便可以检测到不符合的计算机。中央系统健康评估计算机必须对不符合的计算机采取措施。对于不符合的计算机的常见的措施是拒绝其连接网络，但是这种极端的措施不会为不

符合的计算机提供更正其配置状态的机会。

与阻止所有内网的访问相比，更好的允许不符合的计算机更正状态的解决方案，是允许对包含所需更新、软件、脚本或其它资源的内网服务器的子网进行受限访问。例如在受限访问逻辑网络上的服务器包括杀毒或软件更新服务器。通过使用评估系统健康的中央计算机上的资源和基础结构，不符合的计算机可以自动更正其配置。

16.2 部署 NAP 的准备工作

在部署网络访问保护（NAP）之前，需要进行一些准备工作，包括评价当前的网络基础结构和配置独立于 NAP 强制方式的 NAP 组件的设计。在正式进行部署前，需要用户理解基于 Windows 的身份验证基础结构的活动目录的角色、PKI、组策略和 RADIUS 和 NAP 组件和 NAP 强制方式。

16.2.1 评价当前网络基础结构

在开始 NAP 配置之前，需要详细记录和评价当前网络基础结构，以保证其需要的主机和访问服务器，以及保证其满足支持 NAP 的要求。当前网络基础结构的评价可以分为内网计算机、附属内网的第 2 层和网络支持基础结构。

1. 内网计算机

内网计算机可以分为 NAP 客户端的候选对象和不支持 NAP 的客户端，也可以被分为可管理和不可管理两种。

（1）可管理的计算机

可管理的计算机主要分为以下两种方式。

- 支持 NAP：包括运行 Windows Vista、Windows XP SP3 或 Windows Server 2008 的计算机，以及使用 NAP 客户端的其他操作系统；
- 不支持 NAP：包括运行不含有 NAP 客户端的操作系统的计算机。

802.1X 和 VPN 的 NAP 强制方式不需要为健康评估管理计算机，但是身份验证和授权计算机则需要被管理。对于 IPSec 的 NAP 强制方式，计算机可以不被管理，但推荐其接受管理。

（2）不可管理的计算机

不可管理的计算机可以分为以下两种方式：

- 支持 NAP：包括运行 Windows Vista、Windows XP SP3 或 Windows Server 2008 的计算机，以及使用 NAP 客户端的其它操作系统；
- 不支持 NAP：包括运行不含有 NAP 客户端的操作系统的计算机。



2. 附属内网的第 2 层

另外一种计算机的分类是通过附属内网的第 2 层方式。对于有线连接内网的计算机，对桌面用户和服务器计算机，最常用的计算机分类如下：

- 使用 IEEE 802.1X 身份验证：使用 IEEE 802.1X 身份验证鉴别计算机交换端口的使用。如果用户想要使用 802.1X 强制方式，需要确保启用 802.1X 的计算机使用基于 PEAP 身份验证方式，例如 PEAP- MS-CHAP v2 或者 PEAP-TLS。因为系统健康信息是使用 PEAP 消息在有线 NAP 客户端和 NAP 健康策略服务器上传输的，所以需要基于 PEAP 的身份验证方式。如果启用 802.1X 的计算机使用 EAP-MD5-CHAP，需要配置其使用 PEAP-MS-CHAP v2。如果启用 802.1X 的计算机使用 EAP-TLS，需要配置其使用 PEAP-TLS；
- 不使用 802.1X 身份验证：如果用户想要使用 802.1X 强制方式，必须使用 PEAP-MS-CHAP v2 或者 PEAP-TLS 身份验证方式配置 802.1X 身份验证。

对于使用 IEEE 802.11 无线方式连接内网的计算机，最常用的计算机分类如下：

- 使用 IEEE 802.1X 身份验证：使用 WPA2-企业或 WPA-企业和 IEEE 802.1X 标准来认证无线访问点的无线连接的使用。如果用户想要使用 802.1X 强制方式，确保使用 802.1X 的无线客户端计算机使用基于 PEAP 身份验证方式，例如 PEAP- MS-CHAP v2 或者 PEAP-TLS。因为系统健康信息是使用 PEAP 消息在无线 NAP 客户端和 NAP 健康策略服务器上传输的，所以需要基于 PEAP 的身份验证方式。如果无线客户端使用 EAP-TLS，则需要配置其使用 PEAP-TLS；
- 不使用 802.1X 身份验证：如果用户没有使用 WPA2-企业或 WPA-企业的 802.1X 身份验证，立即更新无线网络来保护内网，无论是否想使用 802.1X 强制方式。如果用户想要为无线连接使用 802.1X 强制方式，那么使用基于 PEAP- MS-CHAP v2 或者 PEAP-TLS 身份验证方式的 WPA2-企业或 WPA-企业。

对于使用远程连接内网的计算机，常用形式有便携式计算机从家庭中进行连接，用户可以根据远程访问连接是拨号或 VPN 连接进行分类。由于局域网高速连接的优点，使其发展迅速，对于不符合的计算机远程访问连接不服从于 NAP 健康评估和受限访问的强制。VPN 强制方式不包含拨号远程访问连接。如果用户想要确定所有连接到内网的第二层连接是否服从 NAP 健康评估，需要淘汰拨号远程访问连接。如果不能彻底消除拨号远程访问连接，可以尝试限制拨号远程访问，来降低来自不符合计算机对内网的威胁。

如果想要使用 VPN 强制方式，确保 VPN 客户端计算机正使用基于 PEAP 身份验证方式，例如 PEAP- MS-CHAP v2 或者 PEAP-TLS。因为系统健康信息是使用 PEAP 消息在 VPN 客户端和 NAP 健康策略服务器上传输的，所以需要基于 PEAP 的身份验证方式。

3. 网络支持基础结构

网络支持基础结构是一项在局域网启用网络的服务，具体内容包括如下：

- DHCP：如果想要在基于 Windows 的 DHCP 服务器上使用 DHCP 强制方式，必须更新 DHCP 服务器到 Windows Server 2008；
- DNS：根据如何为不符合的计算机执行受限访问，可能需要其他 DNS 服务器；

- WINS：根据如何为不符合的计算机执行受限访问，可能需要其他 WINS 服务器；
- 活动目录：活动目录域控制器不需要更新到 Windows Server 2008。但根据如何执行受限访问，可能需要其他活动目录域控制器。如果用户的域控制器运行的是 Windows Server 2008，应该为不符合的客户端使用只读域控制器（RODC）。RODC 是 Windows Server 2008 中的一种新型的域控制器，可以配置于不能保障物理安全的位置。RODC 寄宿在活动目录数据库的只读部门；
- 组策略：组策略对象（GPO）可用于集中配置和传播 NAP 客户端设置到可管理的计算机。用户不需要使用 Windows Server 2008 的域控制器。如果所有域控制器运行的都是 Windows Server 2003，则必须在运行 Windows Vista 或 Windows Server 2008 的计算机的 GPO 上配置 NAP 客户端策略设置；
- IPSec：如果用户想要使用 IPSec 强制，用户必须使用连接安全规则的形式更新 IPSec 策略设置，在活动目录 GPO 的 IPSec 身份验证过程中使用健康证书。借助于 NAP 客户端的设置，则不需要使用基于 Windows Server 2008 的域控制器。如果所有域控制器都运行的是 Windows Server 2003，则必须在运行 Windows Vista 或 Windows Server 2008 的计算机的 GPO 上配置 IPSec 策略设置；
- PKI：如果想要使用 IPSec 强制，则必须配置 PKI 或修改现有的 PKI，使其包含基于 Windows 的健康证书颁发结构 CA；
- VPN：如果用户想要使用基于 Windows 的 VPN 服务器的 VPN 强制，则必须更新 VPN 服务器到 Windows Server 2008；
- RADIUS：如果用户没有 RADIUS 基础结构，必须配置基于 Windows Server 2008 的 RADIUS 服务器使用 NAP 强制方式中任意一种。如果用户拥有 RADIUS 基础结构，用户必须更新 RADIUS 服务器到 Windows Server 2008，为 NAP 健康策略评估使用网络策略服务器（NPS）。

16.2.2 相关服务组件的安装

不同类型的 NAP 强制，所需的网络组件有所不同，不仅需要相应的服务器角色，还需要提供辅助验证工作的组件，如证书服务器、域控制器等。通常情况，在网络中应用 NAP 强制之前，首先需要安装或配置相应的服务器角色，然后准备所需的网络环境。

1. 域控制器

域控制器的主要功能就是为内网用户和计算机提供基本的身份认证。在网络中部署和应用 NAP 强制之前，首先应在域中创建相应的用户帐户或组，例如 NAP 免除安全组、测试用户组等。

NAP 免除安全组用于存储网络中的非 NAP 客户端，如 Windows Server 2003、Windows XP（非 SP3）系统用户等。这些用户无法应用各种 NAP 强制，管理员为符合安全策略和不符合安全策略的客户端设置访问权限后，必须单独为这些客户端指定是授权访问，还是限制访问。

测试用户组则用于存储广泛应用 NAP 强制之前的测试工作。不同的 NAP 强制分别限制不同类型的网络访问。如果由于应用了网络健康评估策略，而影响了正常的网络应用，就得不尝试了。因此，应用 NAP 强制之前必需在小范围内进行测试。



2. 证书服务器

数字证书是最常用的网络安全保护手段之一。在部署 NAP 强制的网络中，证书服务器的主要作用，就是为网络中的各种服务器角色或客户端颁发数字证书，实现彼此之间的身份验证。证书服务器在 IPSec 强制的网络中是必需的，而在其他 NAP 强制的网络中则是可选的。例如，在 VPN 强制网络中，如果用户选择了特定的加密传输协议和身份验证方式，则就可能需要准备数字证书，验证 VPN 服务器和 VPN 客户端身份的有效性。

3. 网络策略服务器

网络策略服务器（NPS）是任何 NAP 强制都必需的，提供各种安全健康评估、记账等功能，是 Windows Server 2008 系统的新增功能之一。NPS 允许用户通过 RADIUS 服务器、RADIUS 代理和 NAP 策略服务器，集中配置和管理网络策略。

（1）RADIUS 服务器

从 Windows Server 2008 系统开始，RADIUS 服务器已经被集成在 NPS 中。作为 RADIUS 服务器，NPS 为许多类型的网络访问（包括无线、身份验证切换、VPN 远程访问，路由器到路由器的连接）执行集中化的连接身份验证、授权和记账。

RADIUS 服务器具有对用户帐户信息的访问权限，并可以检查网络访问身份验证凭据。如果用户的凭据是真实的，并且连接尝试获得授权，RADIUS 服务器将根据指定条件向用户授予访问权限，并将网络访问连接记录到记账日志中。使用 RADIUS 允许在一个中心位置（而不是在每台访问服务器上）收集并维护网络访问用户身份验证、授权和记账数据。

（2）RADIUS 代理

作为 RADIUS 代理，NPS 将身份验证和记账消息转发到其他 RADIUS 服务器。使用 NPS，各组织还可以在保留对用户身份验证、授权和记账活动控制的同时，将远程访问基础结构外包给服务提供商。

（3）NAP 策略服务器

NAP 包含在 Windows Vista 和 Windows Server 2008 中，并通过确保按照组织网络健康策略配置客户端计算机后才允许其连接到网络资源，从而有助于保护对专用网络的访问。此外，计算机连接到网络时，NAP 会监视客户端计算机对管理员定义的健康策略的遵从性情况。使用 NAP 自动更新，可以自动更新不符合要求的计算机，以使其遵从健康策略，从而使它们能够连接到网络。

系统管理员可以定义网络健康策略，并使用 NPS 中或其他公司（取决于 NAP 部署）提供的 NAP 组件创建这些策略。

健康策略可以包含软件要求、安全更新要求和所需的配置设置等内容。NAP 通过检查和评估客户端计算机的健康，在认为客户端计算机不健康时限制网络访问以及修正不健康的客户端计算机以进行充分的网络访问，来强制运行健康策略。

16.2.3 更新服务器

当用户配置健康要求策略来强制受限访问时，更新服务器是不符合的 NAP 客户端可以访问的内网的子集。更新服务器包括网络基础结构服务器和健康更新服务器。不符合的 NAP 客户端，使用这些服务器或服务器上的资源来自动或手动执行更新。健康要求策略也可以为不支持 NAP 的客户端强制受限访问。

如果使用报告模式，则不需要更新服务器。在报告模式下，不符合的 NAP 客户端的访问不受限制。但是，为了避免不符合健康要求的计算机为内网带来的为威胁，必须最终转换到强制模式，即需要建立更新服务器。

在 VPN 和 DHCP 模式下不符合的 NAP 客户端，可以访问的更新服务器列表，需要与 NAP 客户端健康评估匹配的网络策略的 NAP 强制设置中，指定的更新服务器组相符合，更新服务器组是一个 IPv4 和 IPv6 地址的列表。该列表应该包括网络基础结构服务器和健康更新服务器。

基础结构服务器包括如下部分：

- DHCP 服务器：为不符合的 NAP 客户端分配 IPv4 地址和其他配置参数，保证其可以访问更新服务器。如果用户正使用 DHCP 强制方式，则不需要添加支持 NAP 的 DHCP 服务器作为更新服务器；
- DNS 和 WINS 服务器：为不符合的 NAP 客户端提供名称解析，保证其可以解析名称，并访问其他更新服务器；
- 活动目录域控制器：保证不符合的 NAP 客户端可以执行域登陆，访问基于域的资源如文件共享；
- Internet 代理服务器：保证不符合的 NAP 客户端可以访问 Internet；
- HRA：保证不符合的 NAP 客户端可以在 IPSec 强制模式下获取健康证书。

更新 NAP 客户端系统健康需要健康更新服务器，包括如下部分：

- 疑难解答 URL 服务器：在“更新服务器和疑难解答 URL”对话框中的疑难解答 URL 文本框中，指定 Web 服务器；
- 反病毒更新服务器：这些服务器可能位于 Internet 上。如果用户拥有 Internet 代理服务器作为更新服务器，则不需要包含基于 Internet 的反病毒更新服务器。如果在内网中拥有反病毒更新服务器，则应该将其作为更新服务器，因为在尝试连接访问基于 Internet 的反病毒服务器前，通常会首先在这些服务器上检查更新；
- 反间谍更新服务器：如同反病毒服务器一样，如果在内网中配置了反间谍更新服务器，则需将其作为更新服务器。如果只存在于 Internet 上，确保 Internet 代理服务器包含在更新服务器组中；
- 软件更新服务器：如同反病毒服务器一样，如果在内网中配置了软件更新服务器，则需将其作为更新服务器。如果只存在于 Internet 上，确保 Internet 代理服务器包含在更新服务器组中。

更新 NAP 客户端所需要的健康更新服务器的设置依赖于用于健康评估的 SHV。



16.3 安装 NPS

在 Active Directory 环境中部署 NAP 系统，用户可以更充分地使用提供的网络访问保护功能。默认安装完成 Windows Server 2008 后，没有安装网络策略和远程访问服务，需要网络用户手动安装该服务。

01 选择“开始”→“服务器管理器”命令，打开“服务器管理器”窗口。选择“角色”选项，在角色窗口中，单击“添加角色”链接，显示“开始之前”对话框。单击“下一步”按钮，显示“选择服务器角色”对话框，选中“网络策略和访问服务”复选框，如图 16.1 所示。

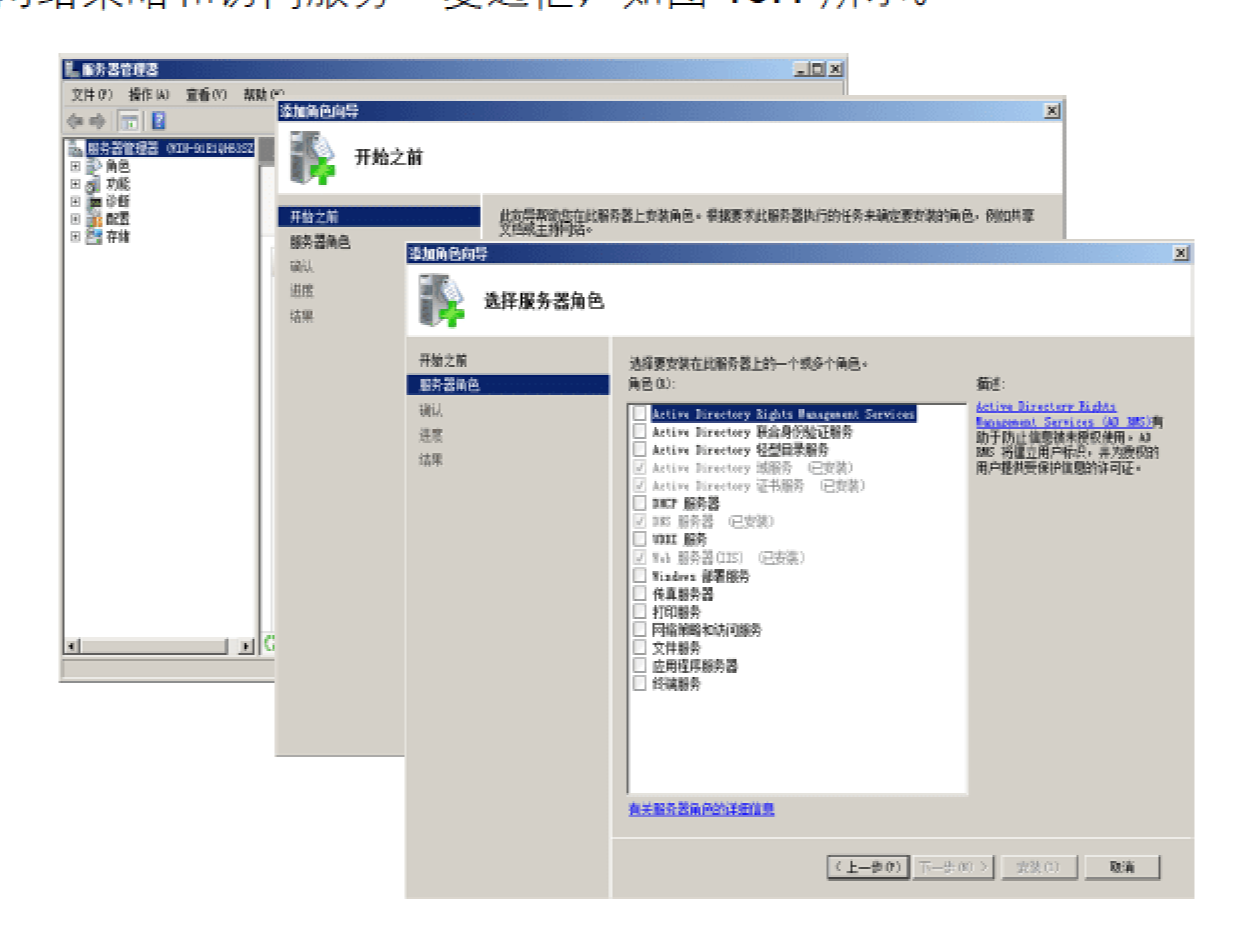


图 16.1 选择服务器角色

02 依次单击“下一步”按钮，查看网络策略和访问服务的相关信息并选择需要安装的角色服务，直至安装完成，如图 16.2 所示。在“角色服务”窗口中，根据下面实验需要选中“网络策略服务器”、“路由和远程访问服务”和“健康注册机构”复选框。

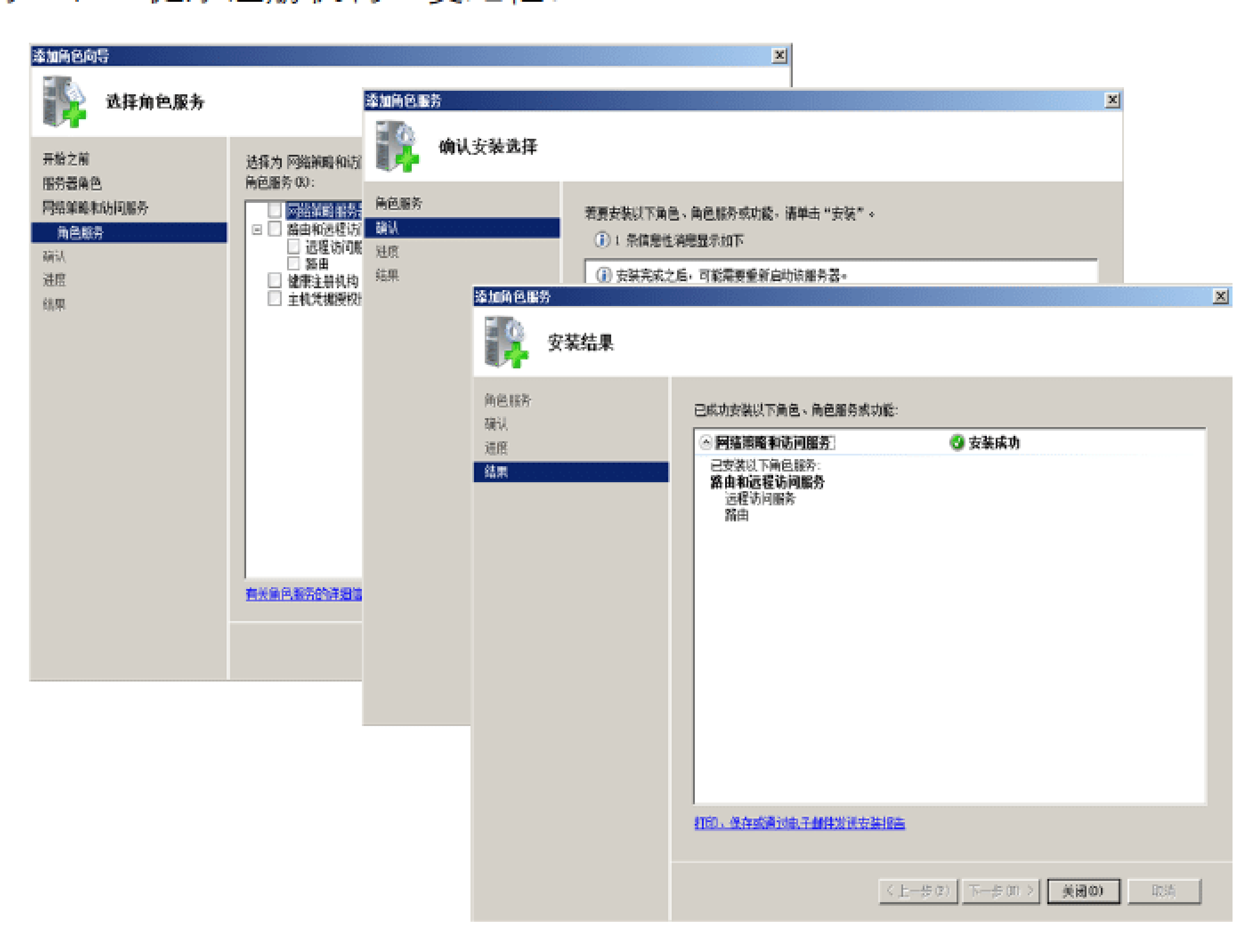


图 16.2 安装网络策略服务器

提示 “路由和远程访问服务”、“健康注册机构”和“主机凭据授权协议”只有特殊环境中才会用到，这里不做选择。如果选择这些角色后需要添加相应的角色服务和功能组件，例如选择“健康注册机构”角色，就需要安装 Active Directory 证书服务、Web 服务器等。

16.4 配置 IPSec 强制

IPSec 强制在网络中界定通信范围，并且保护端到端的通信，建立专门的物理或逻辑链路进行通信。通过 IPSec 强制允许用户为基于 IP 地址、TCP 或 UDP 端口的安全通信设置需求，是 NAP 限制网络访问的最安全和最灵活的方式之一。

16.4.1 IPSec 概述

IPSec 强制通常划分为 3 个逻辑网络（如图 16.3 所示），即安全网络、边界网络和受限网络。计算机在任何时候都只是一个逻辑网络的成员。逻辑网络要求计算机拥有健康证书，而且计算机需要对入站的通信尝试进行身份验证。

- 安全网络。计算机拥有健康证书，入站通信需要尝试使用健康证书认证，为提供 IPSec 保护共享的 IPSec 策略设置；
- 边界网络。计算机拥有健康证书，但对入站通信不需要尝试使用健康证书认证和使用 IPSec 保护。这些类型的计算机都是首先访问和更新 NAP 客户端健康或其他网络服务的服务器。由于编辑网络中的计算机不需要身份验证和受保护的通信，所以必须密切关注他们的健康，防止被利用来攻击安全网络中的计算机；
- 受限网络。NAP 客户端计算机没有完成健康检查即没有健康证书，但仍然需要对所有入站通信尝试使用健康证书认证。这些 NAP 客户端一般式来宾或不支持 NAP 的计算机。

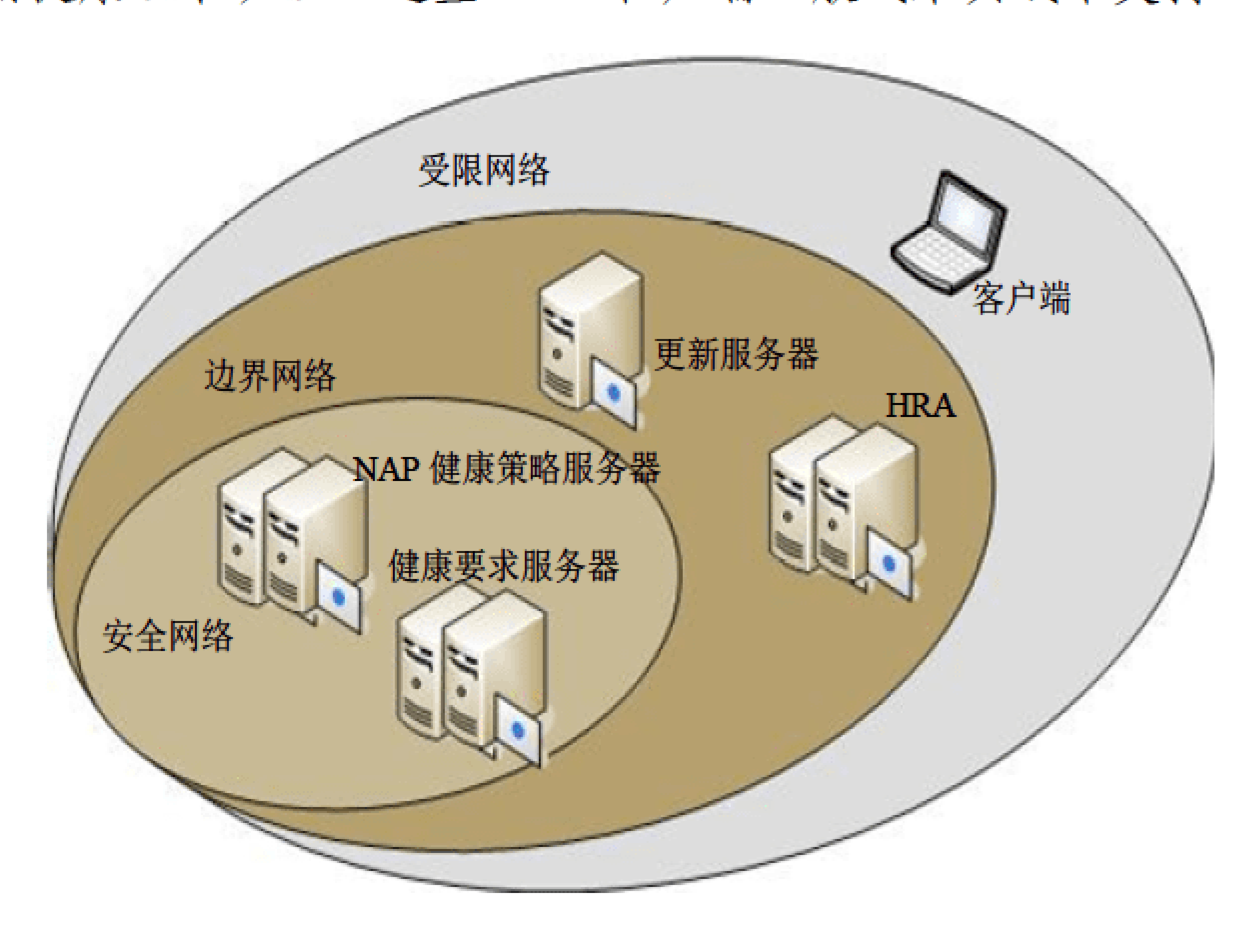


图 16.3 IPSec 强制逻辑网络



16.4.2　配置 CA

CA 在 IPSec 强制系统中起着非常关键的作用，负责为用户计算机颁发健康证书。配置 IPSec 强制之前，如果没有基于 Windows 的 PKI，必须预先配置。对于已有的基于 Windows 的 PKI，必须在证书层的发布 CA 级创建 NAP CA。

1. 创建证书模板

对于基于 Windows Server 2003 的 NAP CA，必须手动创建系统健康身份验证证书模板，保证 IPSec 安全组的成员可以自动注册长生命周期的健康证书。对于基于 Windows Server 2008 的 NAP CA，系统中已经包括了系统健康身份验证证书模板，但是必须确保系统健康身份验证证书模板拥有适当的自动注册的权限。

01 登录证书服务器，依次选择“开始”→“管理工具”→“Certification Authority”命令，打开“certsrv-[证书颁发机构（本地）]”窗口。右击“证书模板”选项，选择快捷菜单中的“管理”命令，打开“证书模板控制台”窗口。右击“工作站身份验证”选项，选择“复制模板”命令，显示如图 16.4 所示“复制模板”对话框，保持默认即可。

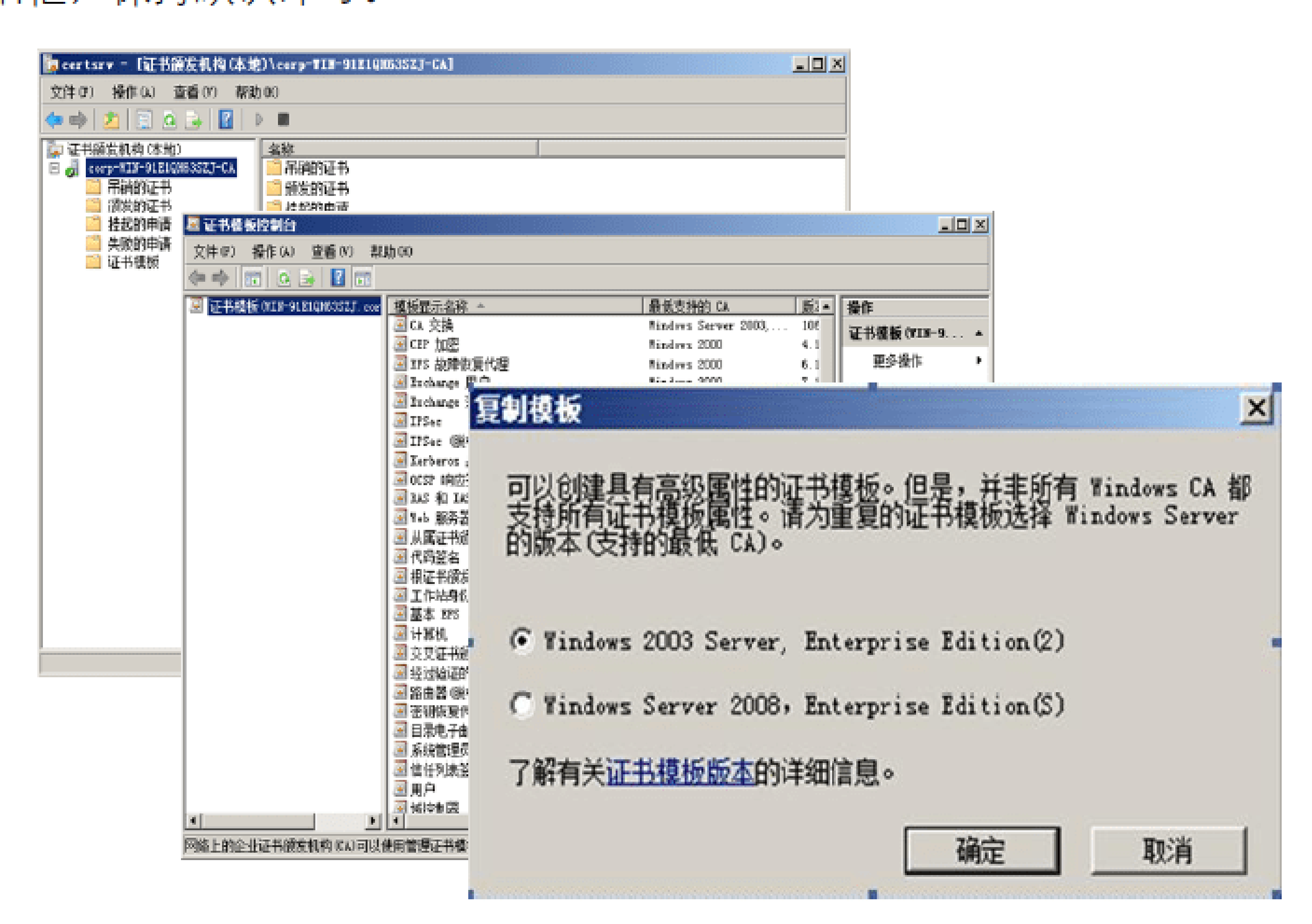


图 16.4　复制模板

02 单击“确定”按钮，显示“新模板的属性”对话框。在“模板显示名称”文本框中输入相应的模板名称，选中“Active Directory 中发布证书”复选框。在“扩展”选项卡中，在“这个模板中包括的扩展”文本框中双击“应用程序策略”选项，显示“编辑应用程序策略扩展”对话框。单击“添加”按钮，显示“添加应用程序策略”对话框，在“应用程序策略”列表中，选择“系统健康身份验证”策略，如图 16.5 所示。依次单击“确定”按钮，返回“新模板的属性”对话框，即可看到“新模板”已经有两个应用程序策略：客户端验证和系统健康身份验证。

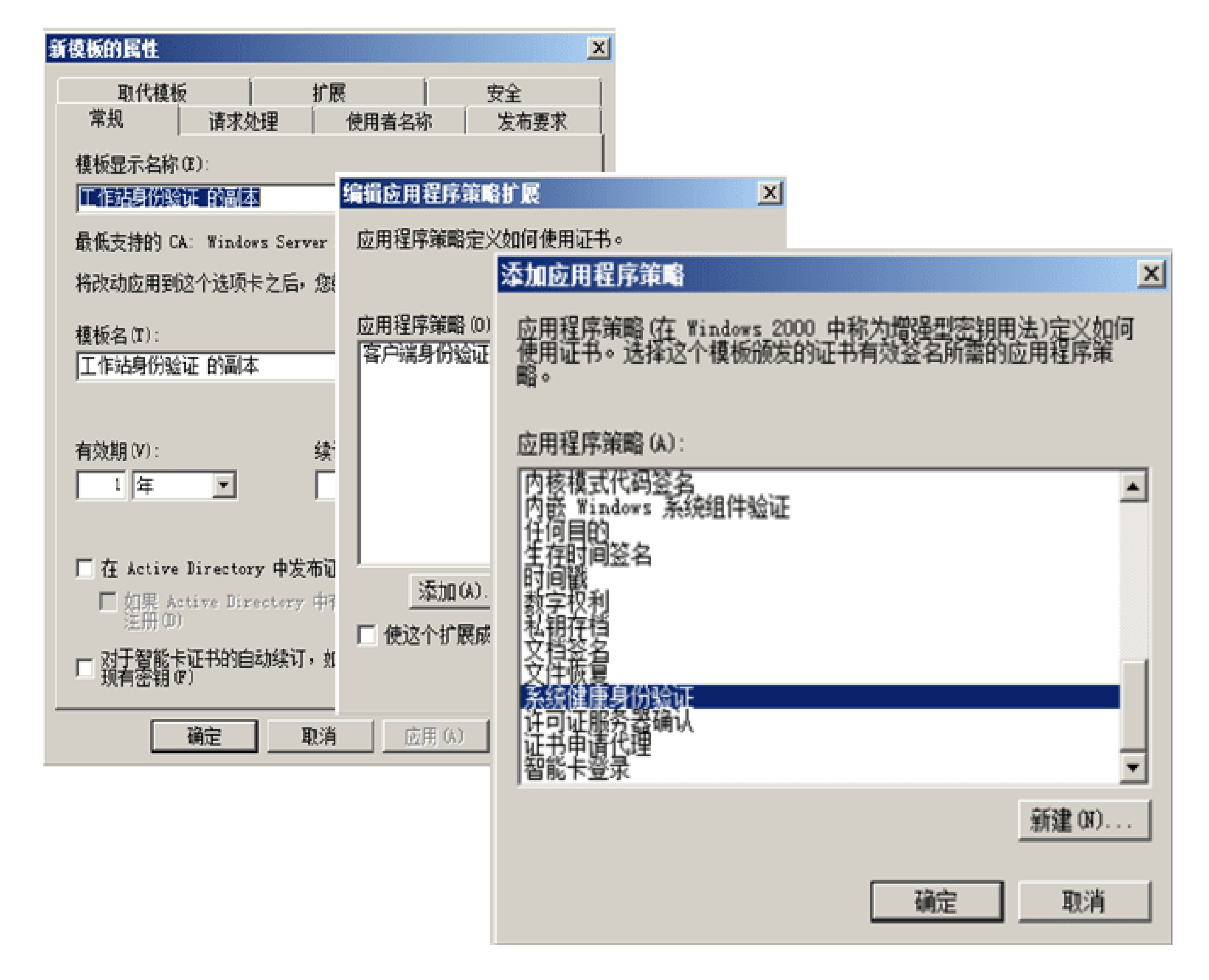


图 16.5 “新模板的属性”对话框

03 在“安全”选项卡中，单击“添加”按钮，显示“选择用户、计算机或组”对话框，输入“company（安全组名称）”。单击“确定”按钮，将其添加到“组或用户名”列表中，选中 company 安全组，在下面“company 权限”权限选项框中选中“注册”和“自动注册”对应的“允许”复选框，如图 16.6 所示。

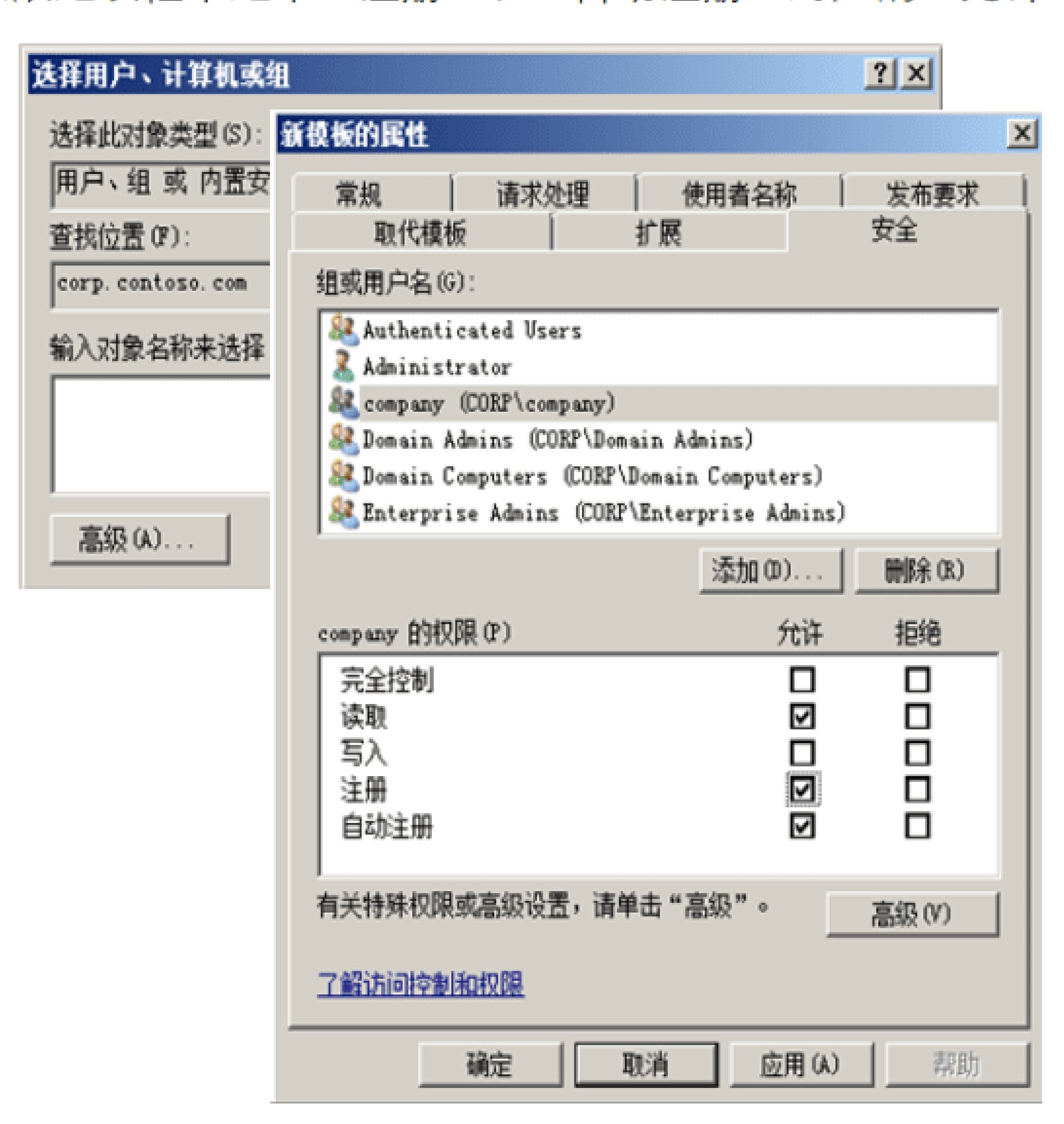


图 16.6 设置安全选项

04 单击“确定”按钮，证书模板创建完成。

2. 颁发证书模板

证书模板创建完成后还需颁发证书模板。在证书颁发机构窗口中，右击“证书模板”选项，选择快捷菜单中的“新建”→“要颁发的证书模板”命令，显示如图 16.7 所示“启用证书模板”对话框。选择“工作站身份验证 的副本”模板，单击“确定”按钮即可。



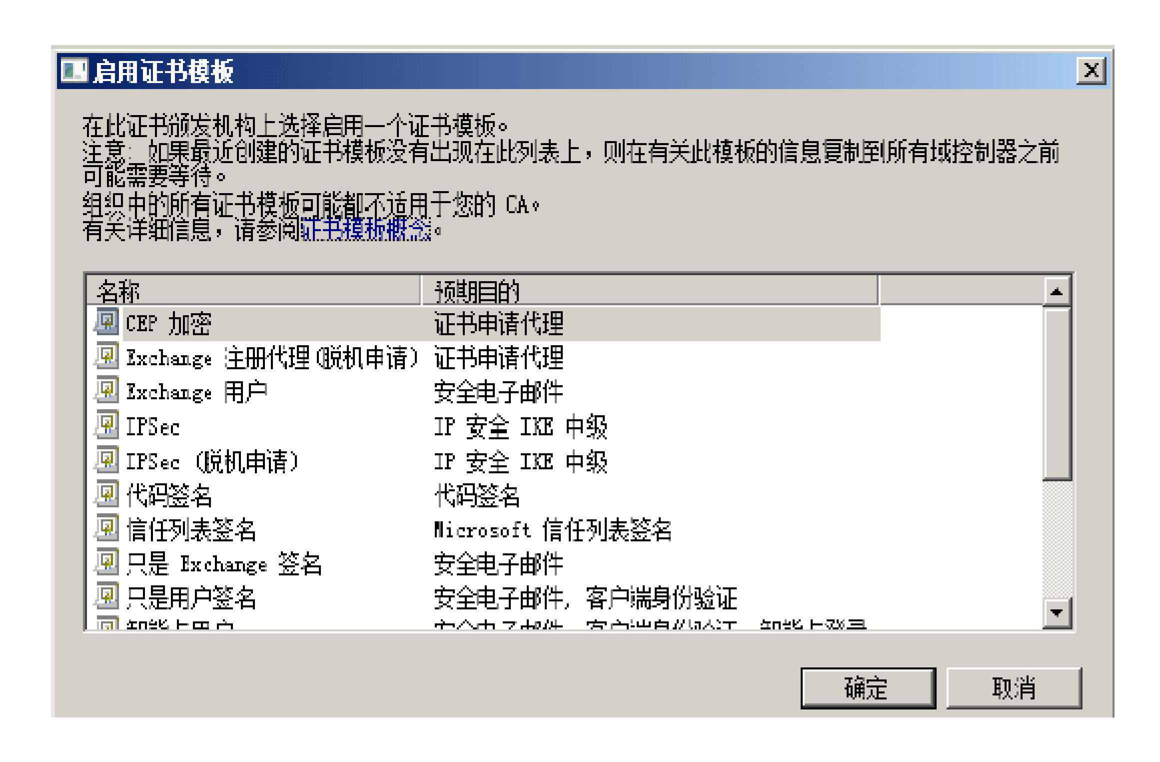


图 16.7　“启用证书模板”对话框

3. 配置 CA 允许非默认的生命周期

企业 CA 必须配置为允许非默认的生命周期，否则符合的 NAP 客户端将被发布健康证书模板指定的生命周期的健康证书，而不是 HRA 配置中指定的短生命周期。

01 登录证书服务器，以管理员帐户打开命令提示符窗口，输入如下命令：

```
certutil.exe -setreg policy\EditFlags +EDITF_ATTRIBUTEENDDATE
```

回车执行，成功完成后显示如图 16.8 所示结果。

```
管理员：命令提示符
C:\Users\Administrator>certutil.exe -setreg policy\EditFlags +EDITF_ATTRIBUTEEN
DDATE
SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\coolpen-LXH-CA\PolicyMod
ules\CertificateAuthority_MicrosoftDefault.Policy\EditFlags:

旧值:
  EditFlags REG_DWORD = 11014e (1114446)
    EDITF_REQUESTEXTENSIONLIST -- 2
    EDITF_DISABLEEXTENSIONLIST -- 4
    EDITF_ADDOLDKEYUSAGE -- 8
    EDITF_BASICCONSTRAINTSCRITICAL -- 40 (64)
    EDITF_ENABLEAKIKEYID -- 100 (256)
    EDITF_ENABLEDEFAULTSMIME -- 10000 (65536)
    EDITF_ENABLECHASECLIENTDC -- 100000 (1048576)

新值:
  EditFlags REG_DWORD = 11016e (1114478)
    EDITF_REQUESTEXTENSIONLIST -- 2
    EDITF_DISABLEEXTENSIONLIST -- 4
    EDITF_ADDOLDKEYUSAGE -- 8
    EDITF_ATTRIBUTEENDDATE -- 20 (32)
    EDITF_BASICCONSTRAINTSCRITICAL -- 40 (64)
    EDITF_ENABLEAKIKEYID -- 100 (256)
    EDITF_ENABLEDEFAULTSMIME -- 10000 (65536)
    EDITF_ENABLECHASECLIENTDC -- 100000 (1048576)
CertUtil: -setreg 命令成功完成。
CertSvc 服务可能需要重新启动，以使更改生效。

C:\Users\Administrator>
C:\Users\Administrator>
```

图 16.8　配置企业 NAP CA

02 运行“net stop certsvc”和“net start certsvc”命令，重启活动目录证书服务，使设置生效，如图 16.9 所示。

```
管理员：命令提示符

C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>net stop certsvc
Active Directory Certificate Services 服务正在停止.
Active Directory Certificate Services 服务已成功停止。


C:\Users\Administrator>net start certsvc
Active Directory Certificate Services 服务正在启动 .
Active Directory Certificate Services 服务已经启动成功。


C:\Users\Administrator>_
```

图 16.9　重启活动目录证书服务

4. 配置健康证书模板的自动注册

为了使边界计算机（IPSec NAP 安全组成员）自动获取长生命周期的健康证书，必须在活动目录中启用证书自动注册。

在“组策略管理编辑器”中，展开“计算机配置\策略\Windows 设置\安全设置\公钥策略”。双击“证书服务客户端 - 自动注册”，显示如图 16.10 所示“证书服务客户端 - 自动注册 属性”对话框。在“配置型号”下拉列表中，选择“已启用”选项，并选中“续订过期证书、更新未决证书并删除吊销的证书”和“更新使用证书模板的证书”复选框。单击“确定”按钮，保存设置即可。

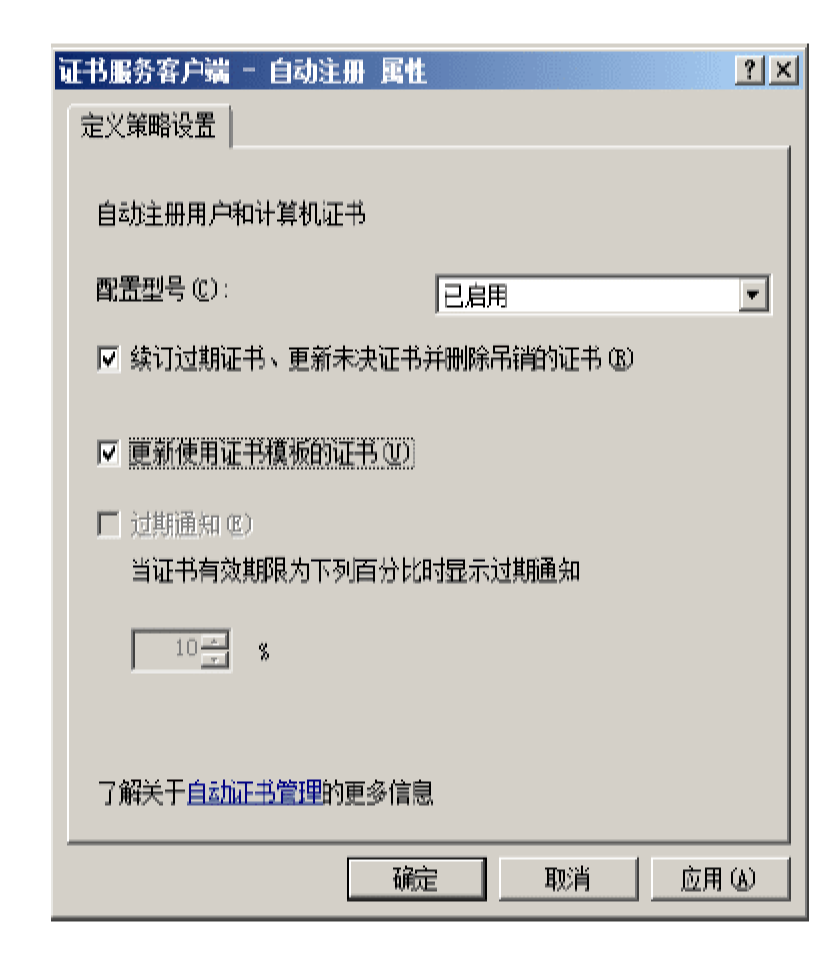


图 16.10　“证书服务客户端-自动注册 属性”对话框

16.4.3　配置域控制器默认策略

通过配置域控制器默认策略可以自动请求客户端颁发验证证书。

01 选择“开始”→“管理工具”→“组策略管理”命令，显示“组策略管理”窗口。依次选择“林：corp.contoso.com”→“corp.contoso.com”→“Default Domain Policy”选项，右击“Default Domain Policy”选项，在弹出的快捷菜单中选择“编辑”命令，打开如图 16.11 所示“组策略管理编辑器”窗口。

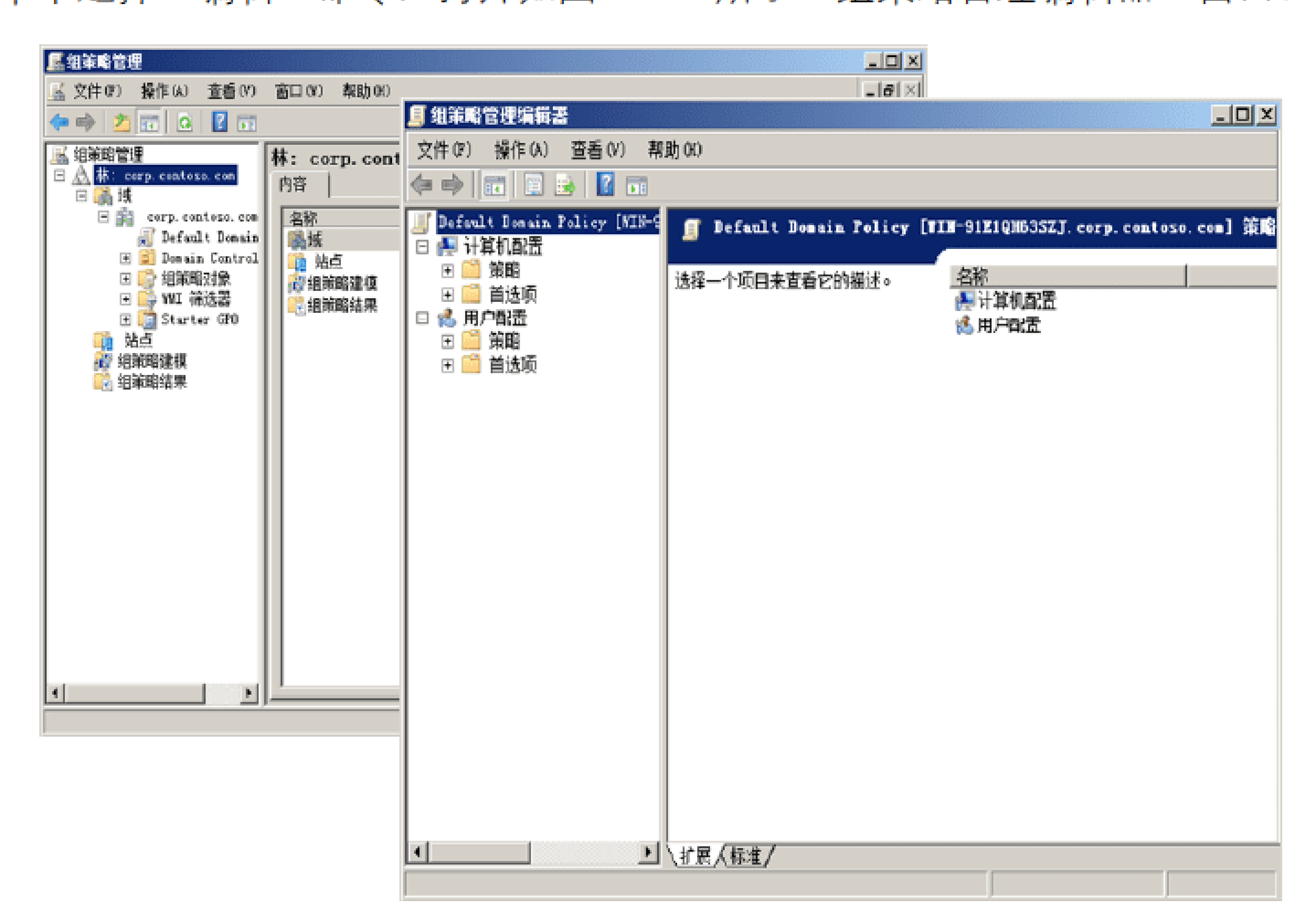


图 16.11　打开“组策略管理编辑器”窗口

02 选择“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“公钥策略”选项，双击“证书客户端 - 自动注册”策略，显示“证书服务客户端 - 自动注册 属性”对话框。在“配置型号”下拉列表框中选中“已启用”选项，同时选中“续订过期证书、更新未决证书并删除吊销的证书”和“更新使用证书模板的证书”复选框，如图 16.12 所示。



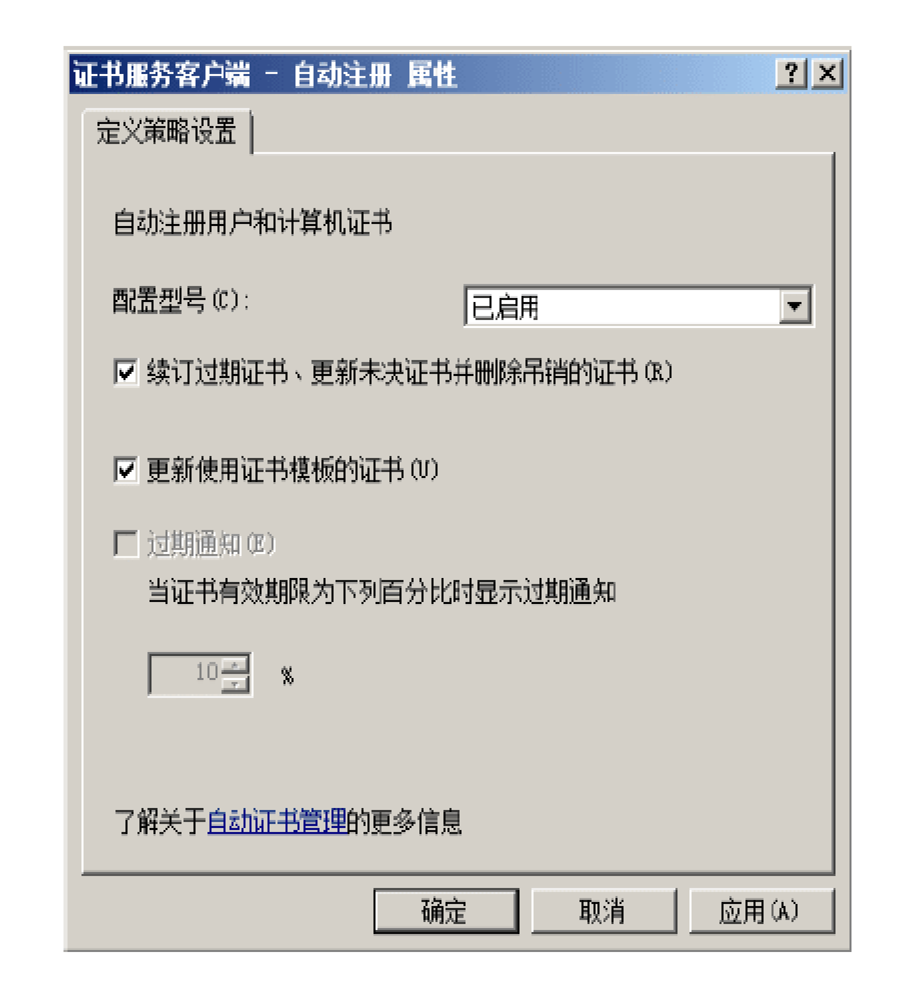


图 16.12　“证书服务客户端 － 自动注册 属性”对话框

03 单击“确定”按钮，完成设置。

16.4.4　配置 NPS

配置 NPS 才能实现网络安全保护，对网络中的计算机进行安全评估。

1. 检查是否获得证书

在 NPS 网络保护环境中，只有获得健康认证的客户端才能访问完了资源。

在控制台窗口中，依次选择“文件”→“添加/删除管理单元”选项，打开“添加或删除管理单元”对话框，选择“证书”选项，单击“添加”按钮，显示“证书管理单元”窗口，选中“计算机帐户”单选按钮。单击“下一步”按钮，在如图 16.13 所示“选择计算机”对话框，选中“本地计算机”单选按钮，单击“完成”按钮，返回“添加或删除管理单元”窗口。

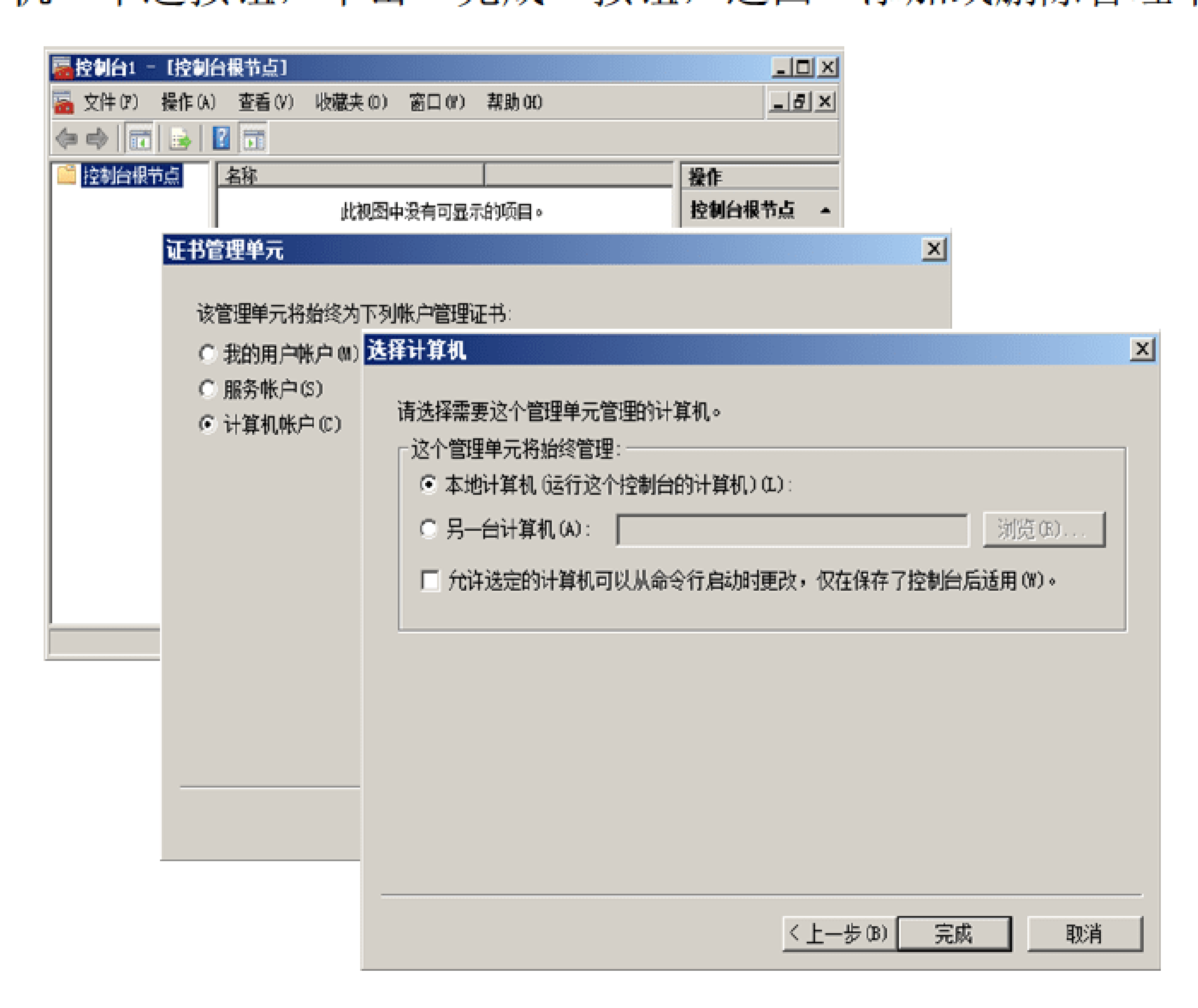


图 16.13　打开“选择计算机”对话框

依次选择“证书（本地计算机）”→“个人”→“证书”选项，就会发现已经从 CA 获得了证书。如果没有获得证书，可能是由于组策略未启用，管理员可以在 NPS 服务器上执行“gpupdate/force”命令，强制刷新组策略。

2. 配置 HRA 属性

通过配置 HRA 来设置健康证书的属性。

01 在 NPS 服务器上，选择“开始”→“管理工具”→“服务器管理器”选项，在打开的“服务器管理器”窗口中，依次选择“角色”→“网络策略和访问服务”→“健康注册机构”→“证书颁发机构”选项。右击“证书颁发机构”选择，在快捷菜单中选择“添加证书颁发机构”命令，显示如图 16.14 所示“添加证书颁发机构”对话框。

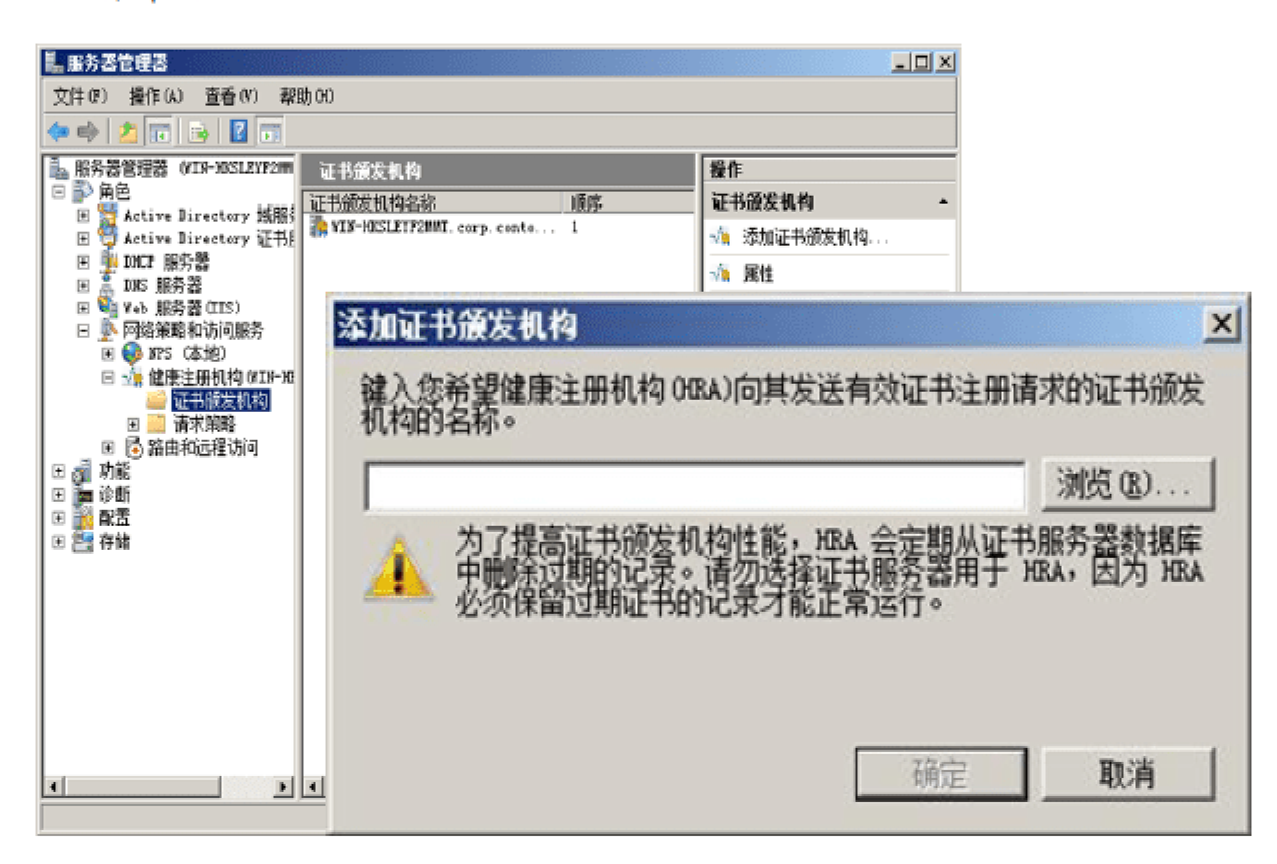


图 16.14　打开“添加证书颁发机构”对话框

02 单击“浏览”按钮，显示“选择证书颁发机构”对话框，选择从 CA 获得的证书。依次单击“确定”按钮，将其添加到“服务器管理器”窗口中，右击“证书颁发机构”选项，在弹出的快捷菜单中选择“属性”命令，显示如图 16.15 所示“证书颁发机构属性”对话框，设置 HRA 要求的健康证书的有效时间和 HRA 是否使用独立或企业 CA。

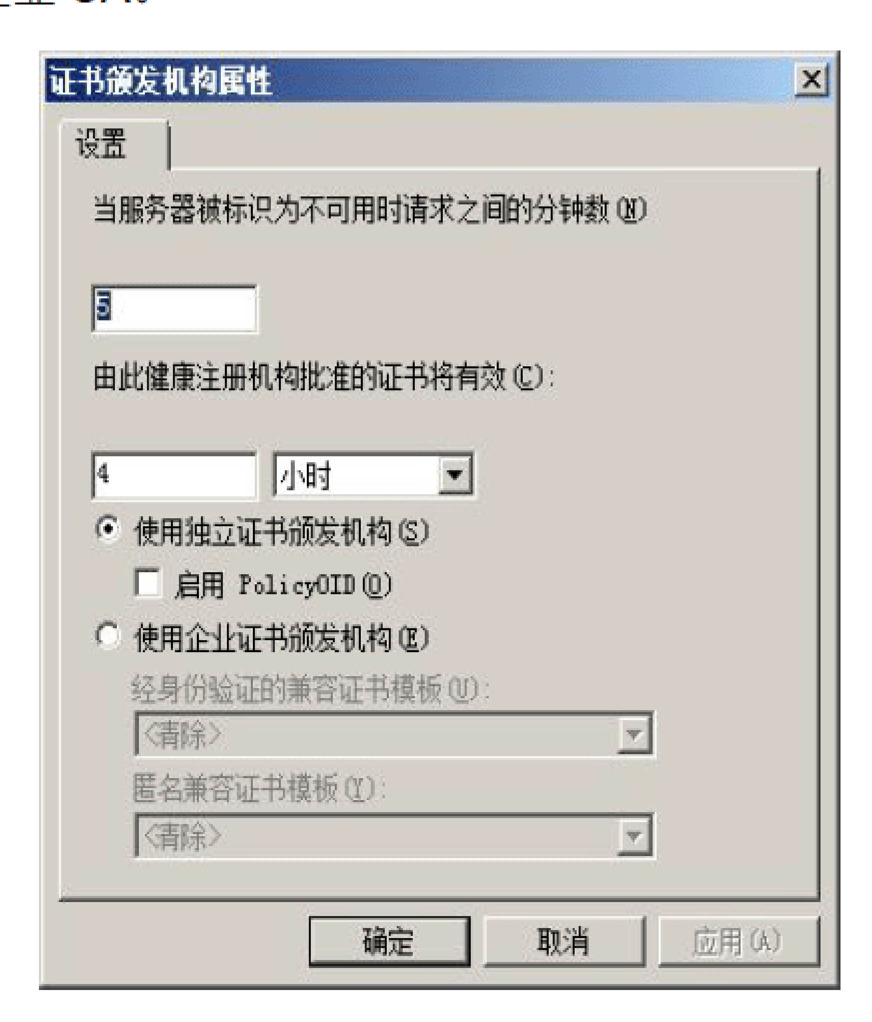


图 16.15　“证书颁发机构属性”对话框



03 单击“确定”按钮，即可完成配置。

3. 在 CA 上赋予 NPS 计算机帐户相应权限

NPS 服务器要为符合健康策略的计算机颁发证书和删除证书，所以 HRA 必须要有“请求”、“发送”和“管理证书”的权限。

01 在证书颁发机构中，右击“证书服务器（以 corp-WIN-91E1QH63SZJ-CA 为例）”选项，选择快捷菜单中的“属性”命令，显示“corp-WIN-91E1QH63SZJ-CA 属性”对话框。切换至“安全”选项卡，单击“添加”按钮，显示如图 16.16 所示“选择用户、计算机或组”对话框，将 NPS 对应的计算机帐户添加到安全帐户列表中。

02 单击“确定”按钮，返回“安全”选项卡，选中 NPS 对应的计算机帐户，在“组或用户名”选项框中赋予其“颁发和管理证书”、“管理 CA”和“请求证书”权限，如图 16.17 所示。





图 16.16　打开“选择用户、计算机或组”对话框

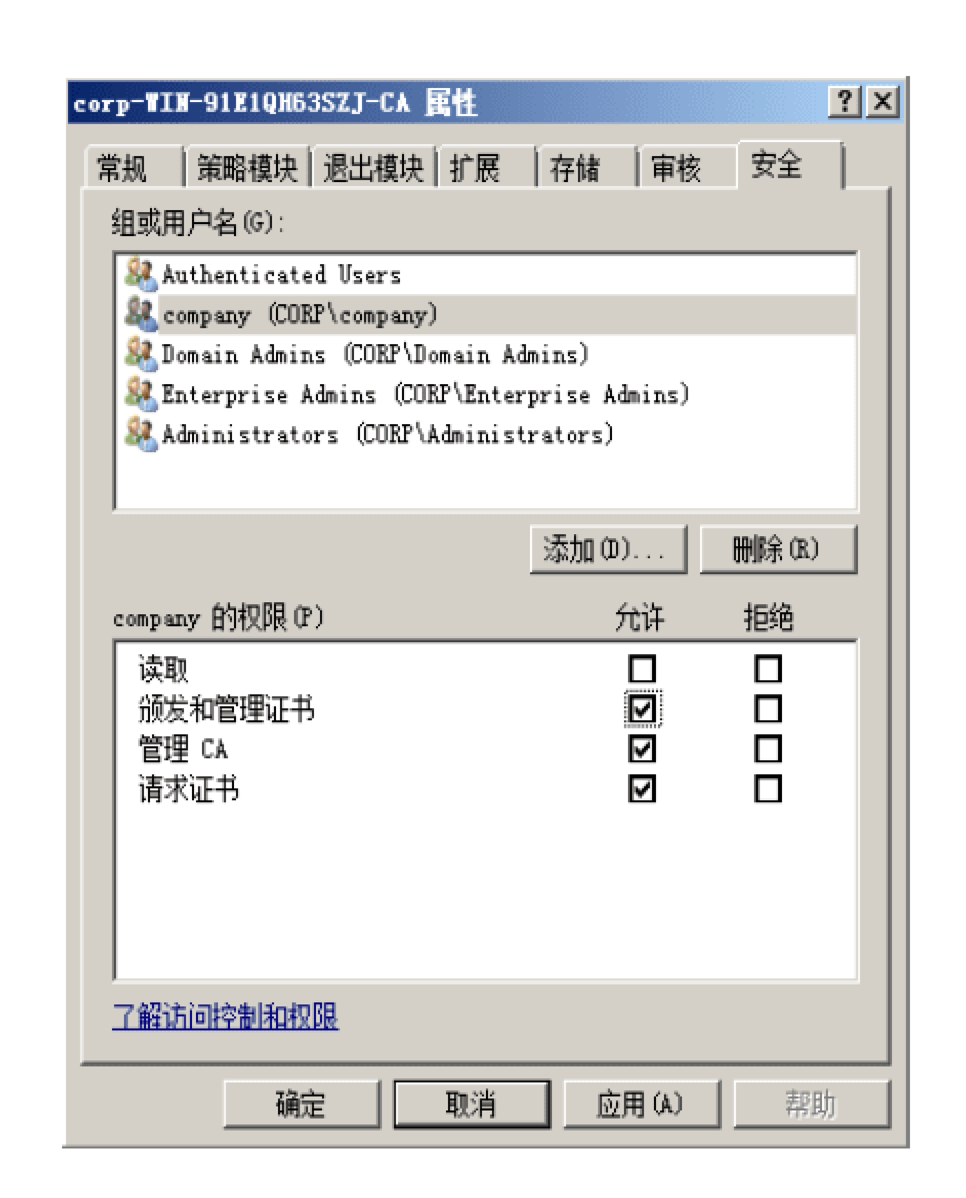


图 16.17　“安全”选项卡

03 单击“确定”按钮，完成配置。

4. 配置网络策略服务器

通过 NPS 向导可快速配置 IPSec 强制健康要求策略。

01 在 NPS 服务器上，选择“开始”→“管理工具”→“网络策略服务器”命令，显示“网络策略服务器”窗口。单击“配置 NAP”连接，显示如图 16.18 所示“选择与 NAP 一起使用的网络连接方法”对话框，在“网络连接方法”下拉列表框中，选择“带有健康注册机构（HRA）的 IPSec”选项。

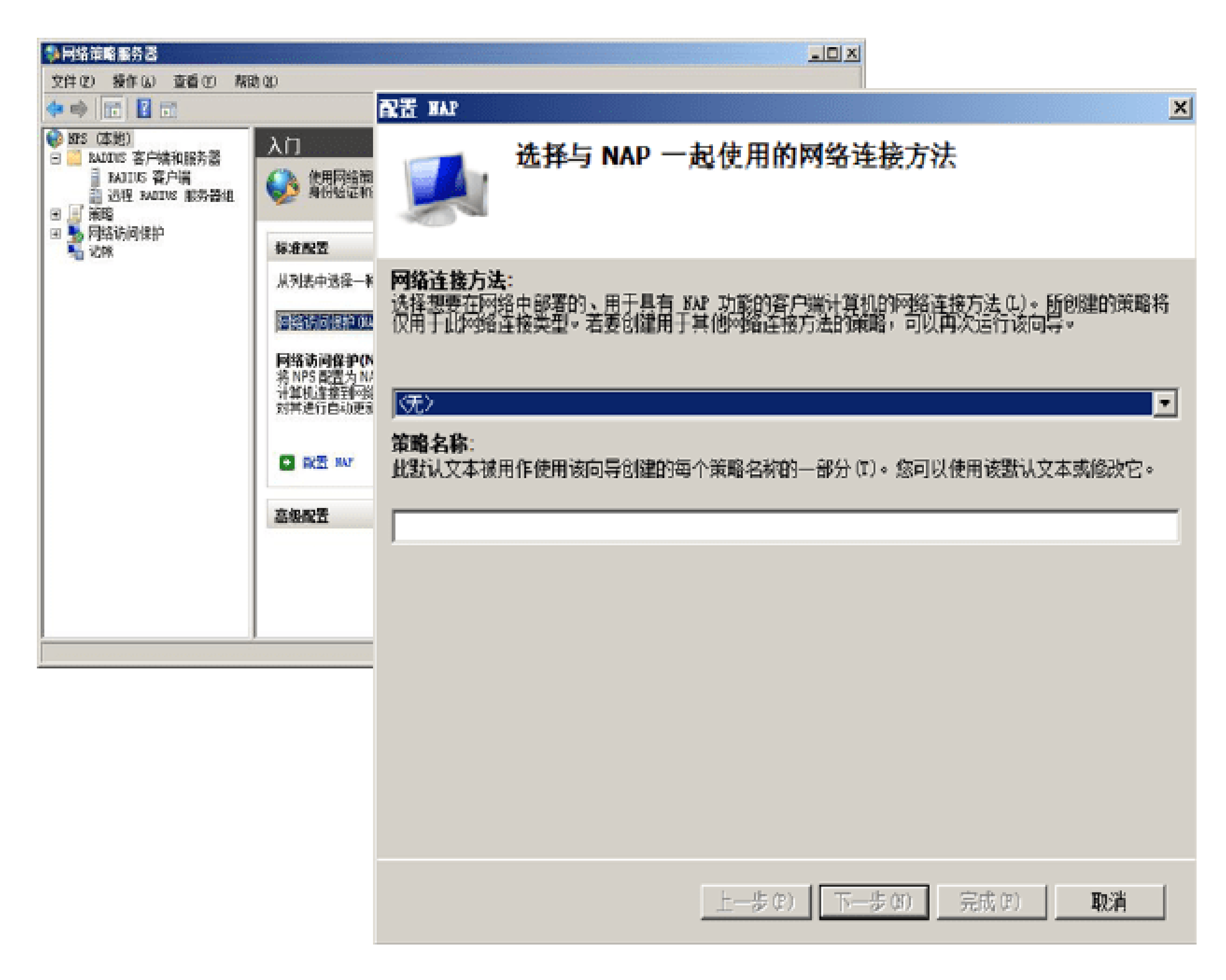
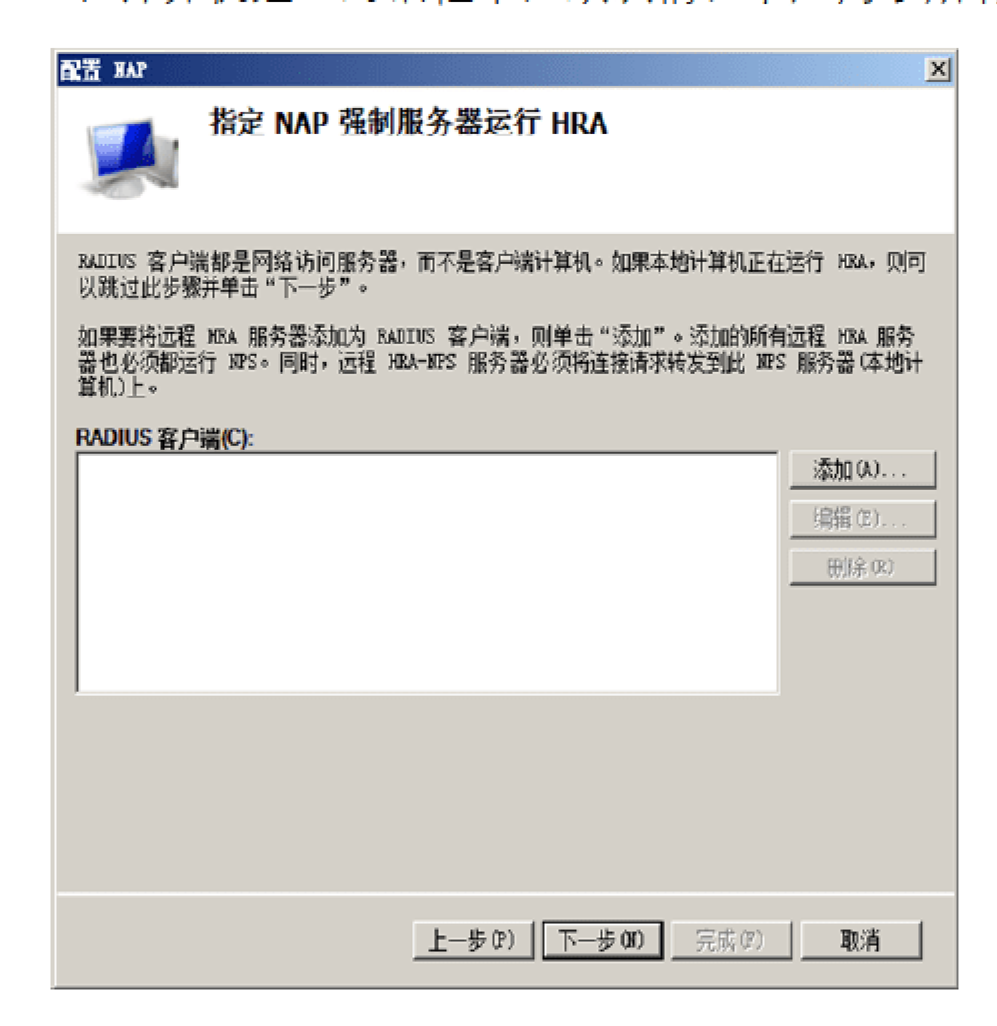


图 16.18　打开“选择与 NAP 一起使用的网络连接方法”对话框

02 依次单击“下一步”按钮，配置 RADIUS 客户端和计算机组，如图 16.19 所示。在“指定 NAP 强制服务器运行 HRA”对话框中，本例是在本地计算机上运行 HRA，所以可以跳过此步骤。在“配置用户组和计算机组”对话框中，默认情况下应用于所有用户组和计算机组。



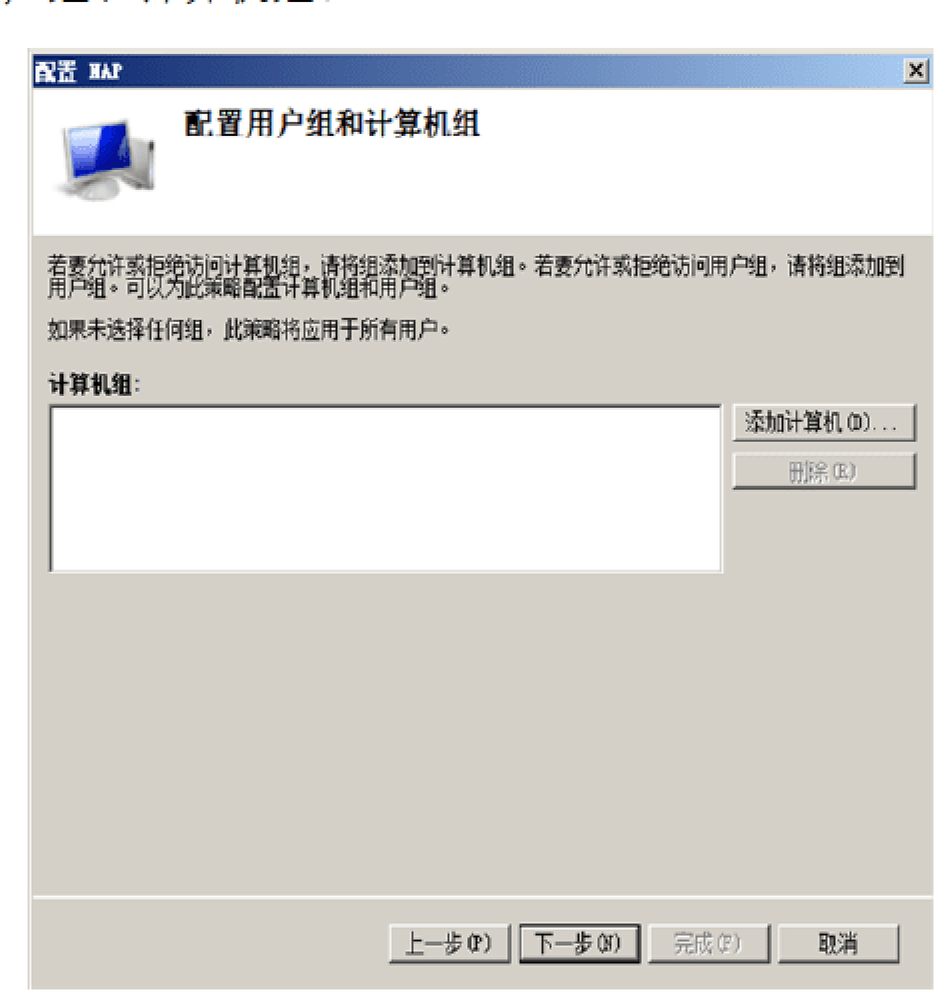


图 16.19　配置 RADIUS 客户端和计算机组

03 依次单击“下一步”按钮，定义 NAP 健康策略和确认策略配置，如图 16.20 所示。在“定义 NAP 健康策略”对话框中，选中“Windows 安全健康验证程序”和“启用客户端计算机的自动更新”复选框。在“正在完成 NAP 增强策略和 RADIUS 客户端配置”对话框中，检查当前配置清单，是否需要修改。



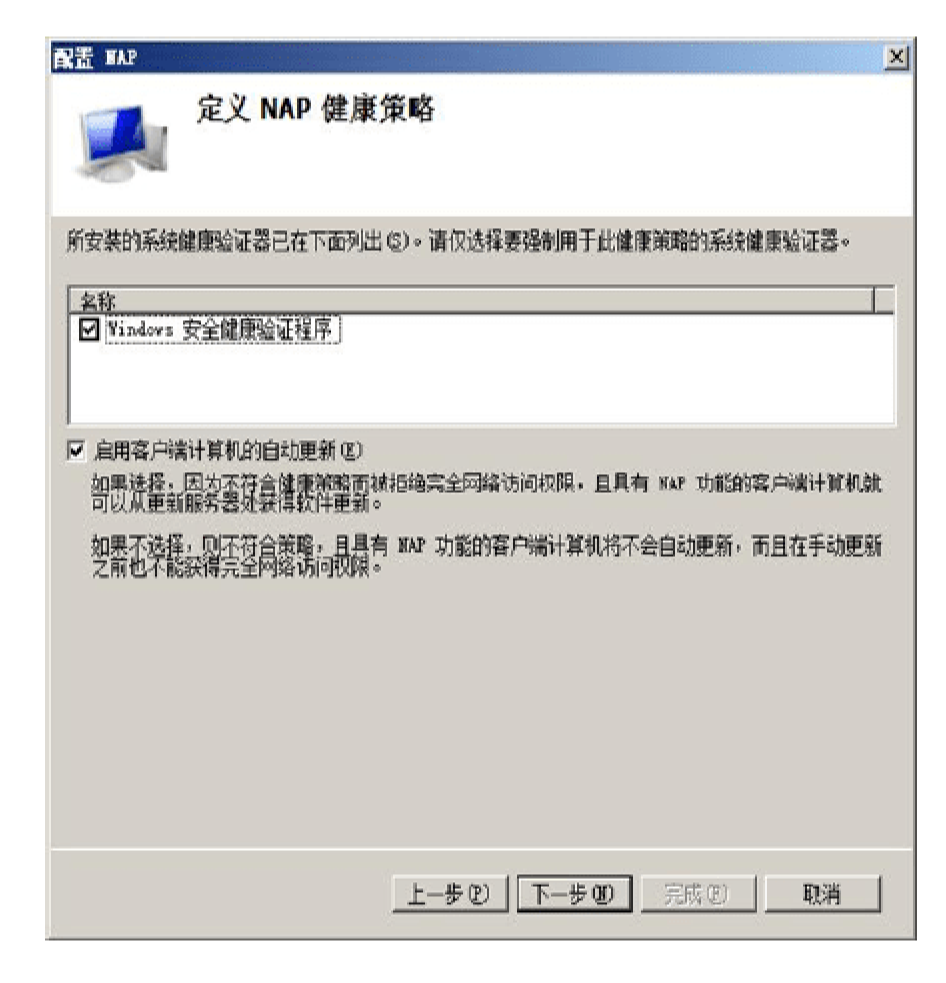




图 16.20　定义 NAP 健康策略和确认策略配置

04 单击“完成”按钮，完成 NAP 向导配置。

5. 配置 SHV

SHV 的配置是由客户端健康要求决定的，Windows 安全健康验证程序包括防火墙、自动更新、防病毒程序、防间谍软件等审核对象。

01 在网络策略服务器中，选择“网络访问保护”→“系统健康验证器”选项，如图 16.21 所示。

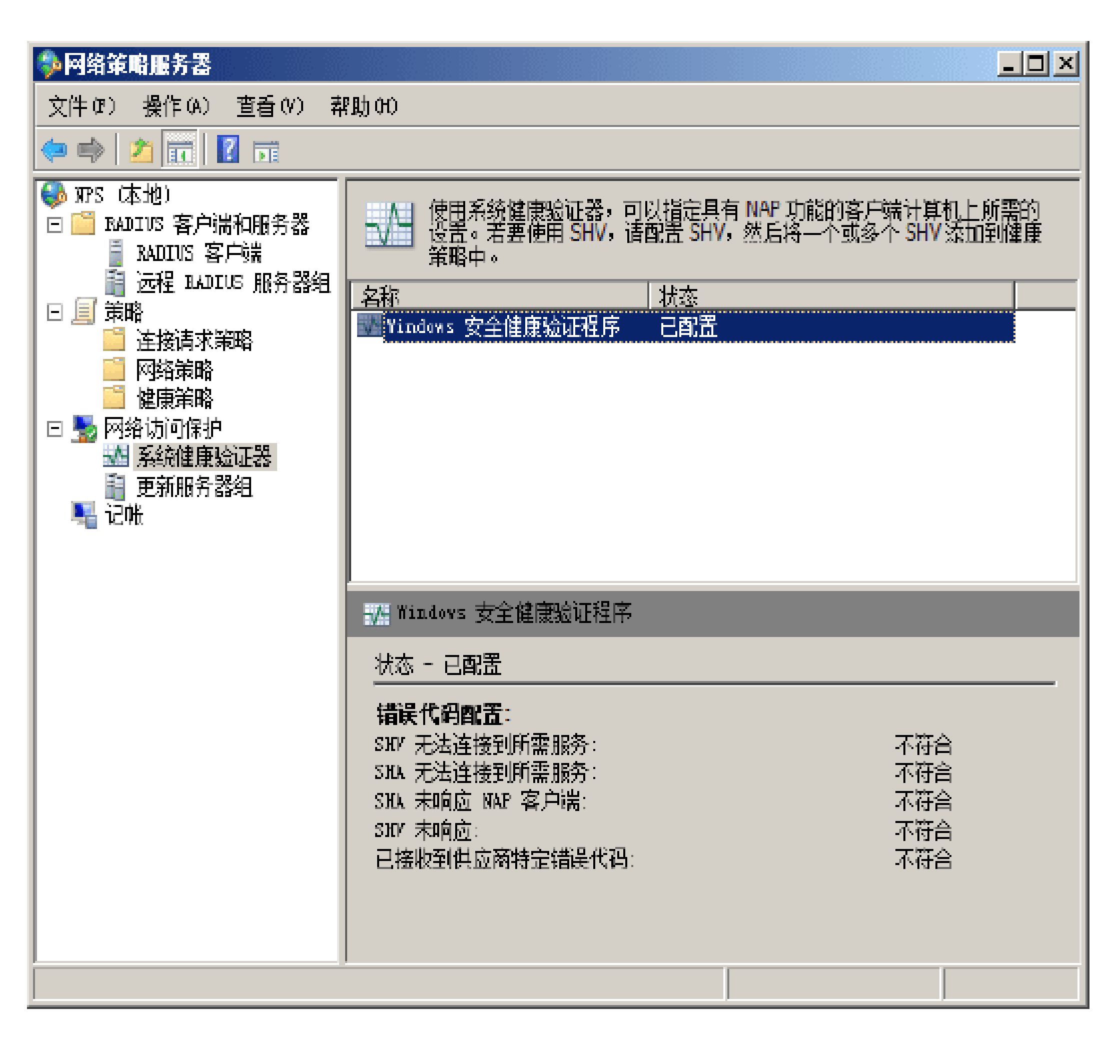


图 16.21　“系统健康验证程序”窗口

02 双击“Windows 安全健康验证程序”选项，显示“Windows 系统健康验证程序 属性”对话框，根据系统健康要求配置 SHV。单击“配置”按钮，显示如图 16.22 所示“Windows 安全健康验证程序”对话框，选中需要进行健康检查内容的复选框。



图 16.22　Windows 系统健康验证程序

03 单击“确定”按钮，保存设置并退出。

16.4.5　配置 IPSec 强制客户端

尽管可以单独配置 NAP 客户端，但是在活动目录域环境中，建议使用集中配置 NAP 客户端的方式，通常情况下是通过组策略设置，主要包括如下任务：

- 配置 NAP 客户端设置；
- 启用 Windows 安全中心；
- 配置网络访问保护代理服务的自动启用。

1. 配置 NAP 客户端的设置

01 在“组策略管理器”管理单元中，依次展开“林”→“域”。在“连接的组策略对象”面板中，右击组策略对象（默认对象是 Default Domain Policy），在快捷菜单中选择“编辑”选项，打开“组策略管理编辑器”窗口。

02 依次展开“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“Network Access Protection”→“NAP 客户端配置”→“强制客户端”选项，双击“IPSec 信赖方”强制客户端，显示如图 16.23 所示“IPSec 信赖方 属性”对话框，选中“启用此强制客户端”复选框。单击“确定”按钮，保存设置。



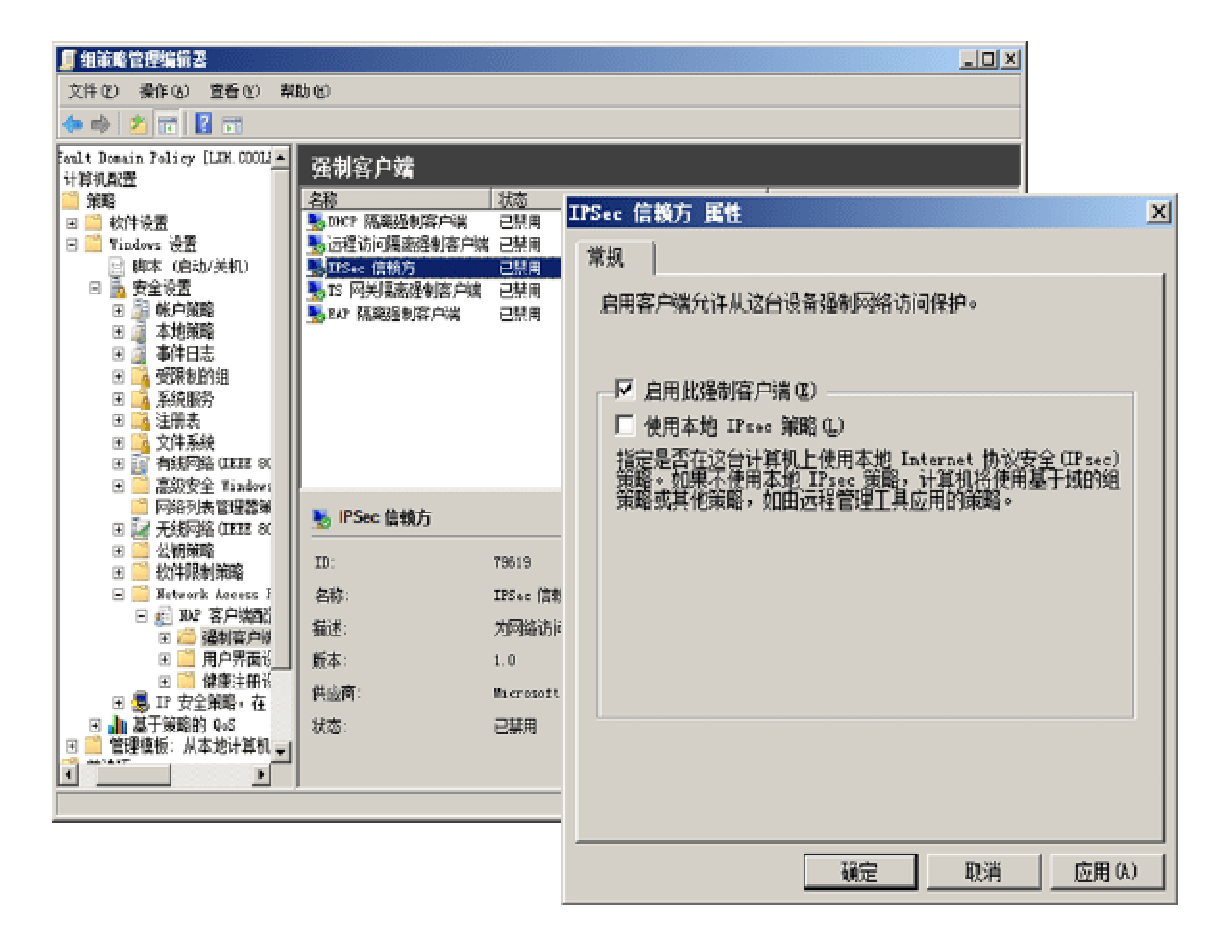


图 16.23 打开“IPSec 信赖方 属性”对话框

03 如果使用受信任的服务器组作为 NAP 客户端查找 HRA 的方法，可在控制树中展开“健康注册设置”，如图 16.24 所示。

04 添加受信任服务器组。右击“受信任服务器组”，在快捷菜单中选择“新建”选项，显示如图 16.25 所示“组名”对话框。在“组名”文本框中，输入组的名称。



图 16.24 展开“健康注册设置”

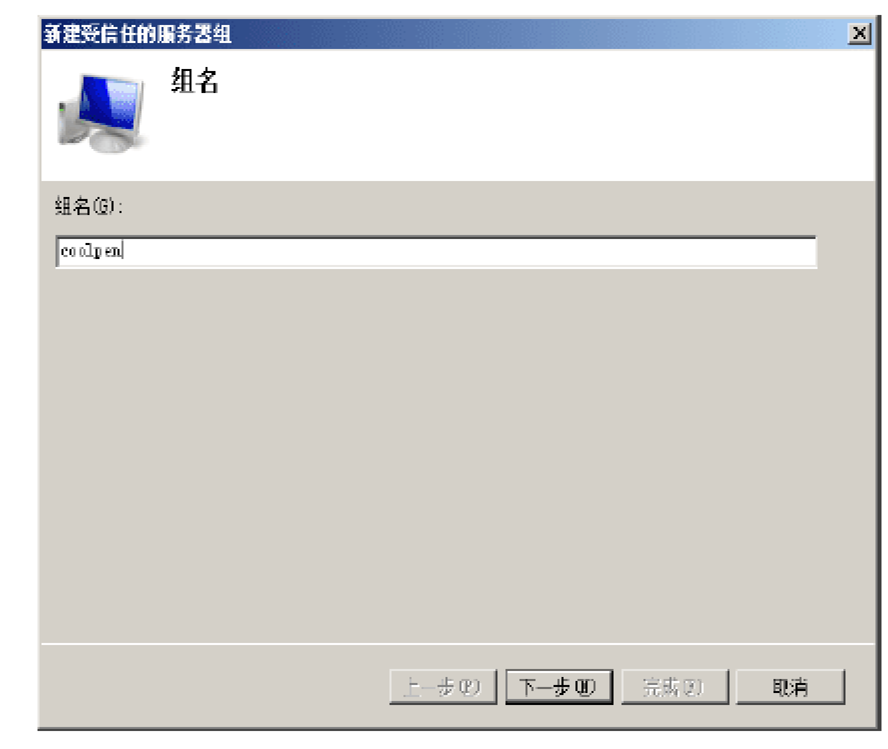


图 16.25 “组名”对话框

05 单击“下一步”按钮，显示如图 16.26 所示“添加服务器”对话框。根据需要在“添加您希望客户端信任的注册机构的 URL”文本框中，输入为应用组策略对象的 NAP 客户端所使用的 HRA 添加 URL。

- 为使用 SSL 的 HTTP 认证健康证书，URL 必须以如下形式：

https://HRA_FQDN/domainhra/hcsrvext.dll，其中 HRA_FQDN 为 HRA 计算机的 FQDN；

- 为认证使用 HTTP 的健康证书，URL 必须采用如下形式：

http://HRA_FQDN/domainhra/hcsrvext.dll；

- 为认证使用通过 SSL 的 HTTP 的匿名健康证书，URL 必须采用如下形式：

https://HRA_FQDN/nondomainhra/hcsrvext.dll；

- 为认证使用 HTTP 的匿名健康证书，URL 必须采用如下形式：

http://HRA_FQDN/nondomainhra/hcsrvext.dll。

06 如果想要所有 URL 都基于 SSL，需要选中“要求对此组中的所有服务器进行服务器验证（http:）”复选框。如果任意一个 URL 不是基于 SSL 的，清除“要求对此组中的所有服务器进行服务器验证（http:）”复选框即可，如图 16.27 所示为当所有 URL 都是基于 SSL 的实例。验证列表中的所有 URL 是否按照正确的顺序，如不正确，可以单击“上移”、“下移”按钮来更正。



图 16.26 “添加服务器”对话框

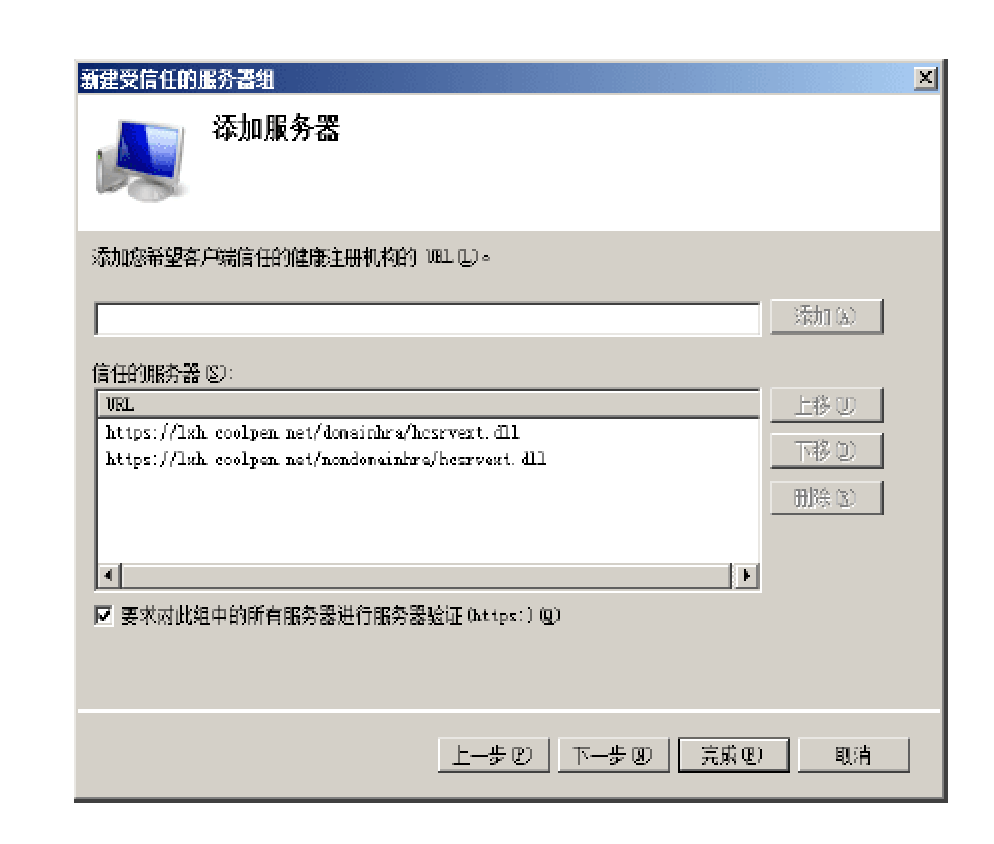


图 16.27 配置基于 SSL 的 URL 的实例

07 单击“下一步”按钮，显示“正在完成受信任的服务器组向导”对话框。单击“完成”按钮，完成添加受信任服务器组的操作。

2. 启用 Windows 安全中心

为了使用组策略启用 NAP 客户端上的 Windows 安全中心，可按如下步骤操作：

在“组策略管理”管理单元中，依次展开“计算机配置”→“策略”→“管理模板”→“Windows 组件”→“安全中心”，如图 16.28 所示。双击“启用安全中心（仅限域 PC）”，显示“启用安全中心（仅限域 PC）属性”对话框，选择“已启用”单选按钮。最后，单击“确定”按钮，保存设置即可。

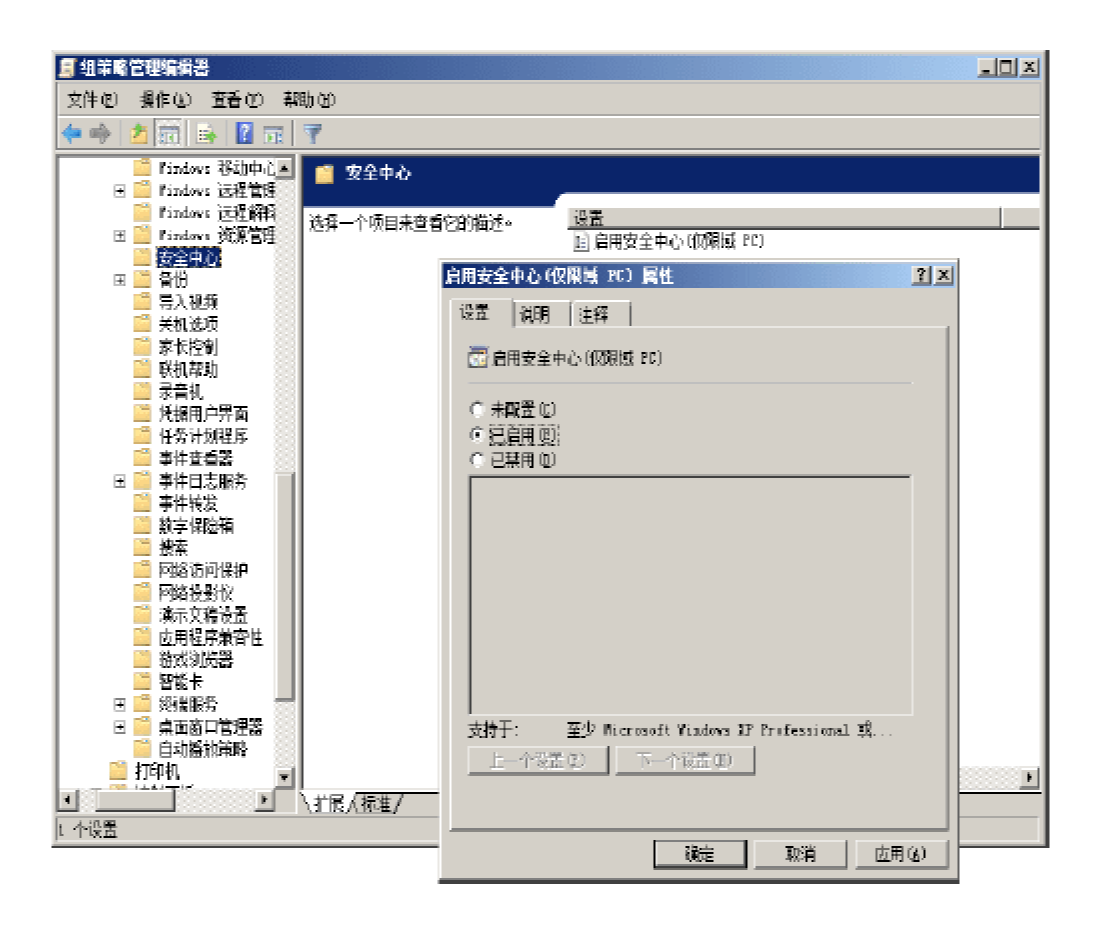


图 16.28 启用安全中心



3. 配置网络访问保护代理服务的自动启用

01 在“组策略管理”管理单元中，依次展开“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“系统服务”。在详细面板中，双击“Network Access Protection Agent”，显示如图 16.29 所示“Network Access Protection Agent 属性”对话框。选中“定义这个策略设置”复选框，并选择“自动”单选按钮。

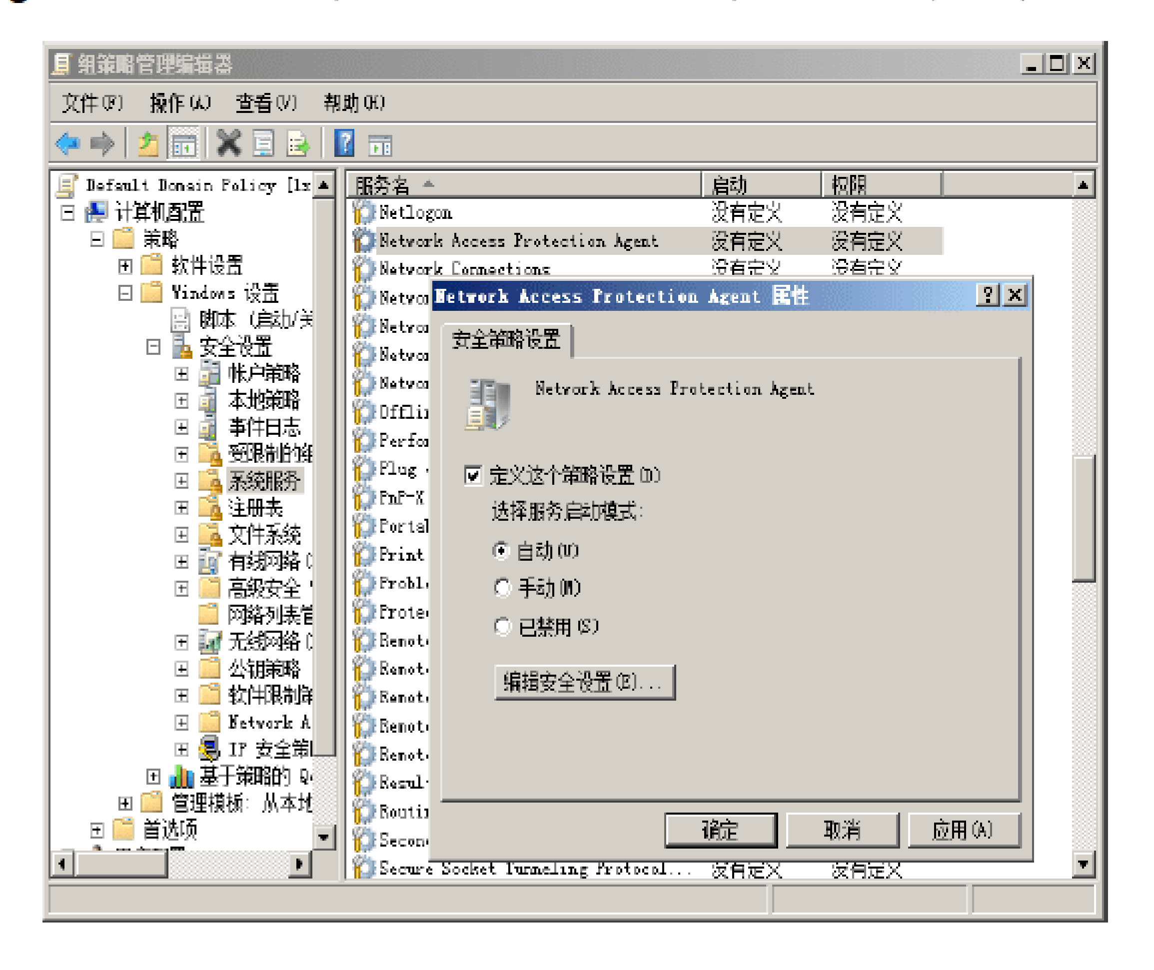


图 16.29　打开“Network Access Protection Agent 属性”对话框

02 单击“确定”按钮，保存设置。

16.4.6　应用 IPSec 策略设置

将 IPSec 强制安全策略应用到网络之前，必须先在实验环境中进行测试，确认生效后方可大规模应用。NPS 会对登录域的客户端计算机进行健康评估，如果符合策略要求，可以正常使用网络中的资源，否则将被隔离，直至恢复健康状态。除此之外，IPSec 强制还可以与 Windows 高级防火墙配合使用，用户实现特定的端到端安全通信，适合安全较高的网络访问。

01 在 Windows Server 2008 域控制器上，打开指定 GPO 的“组策略管理编辑器”窗口，依次展开“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“高级安全 Windows 防火墙”→“高级安全 Windows 防火墙-LDAP”，如图 16.30 所示。

02 右击“高级安全 Windows 防火墙-LDAP”，在快捷菜单中选择“属性”选项，显示如图 16.31 所示“高级安全 Windows 防火墙-LDAP 属性”对话框。在“域配置文件”选项卡中，在“防火墙状态”下拉菜单中选择“启用（推荐）”选项，在“入站连接”下拉菜单中选择“阻止（默认值）”选项，在“出站连接”下拉菜单中选择“允许（默认值）”选项。单击“确定”按钮，保存配置。

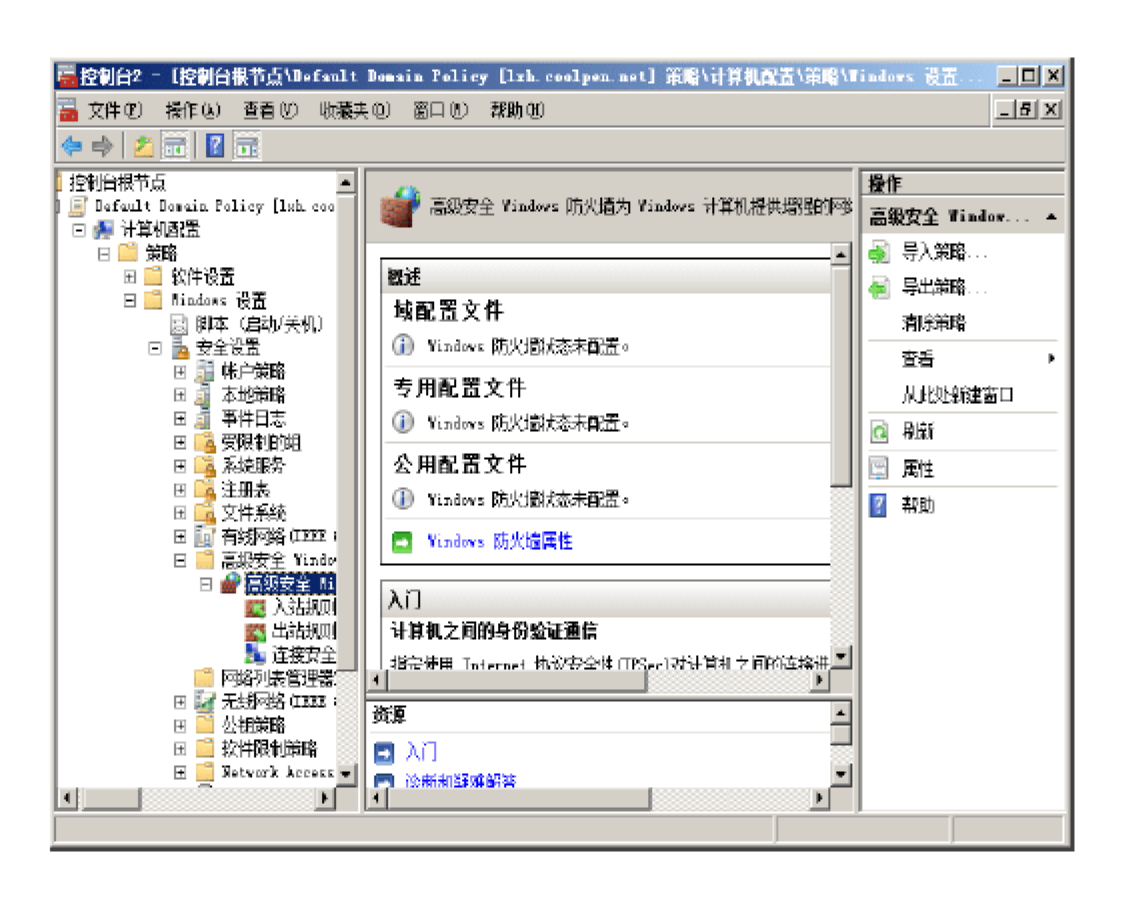


图 16.30　展开“高级安全 Windows 防火墙-LDAP”

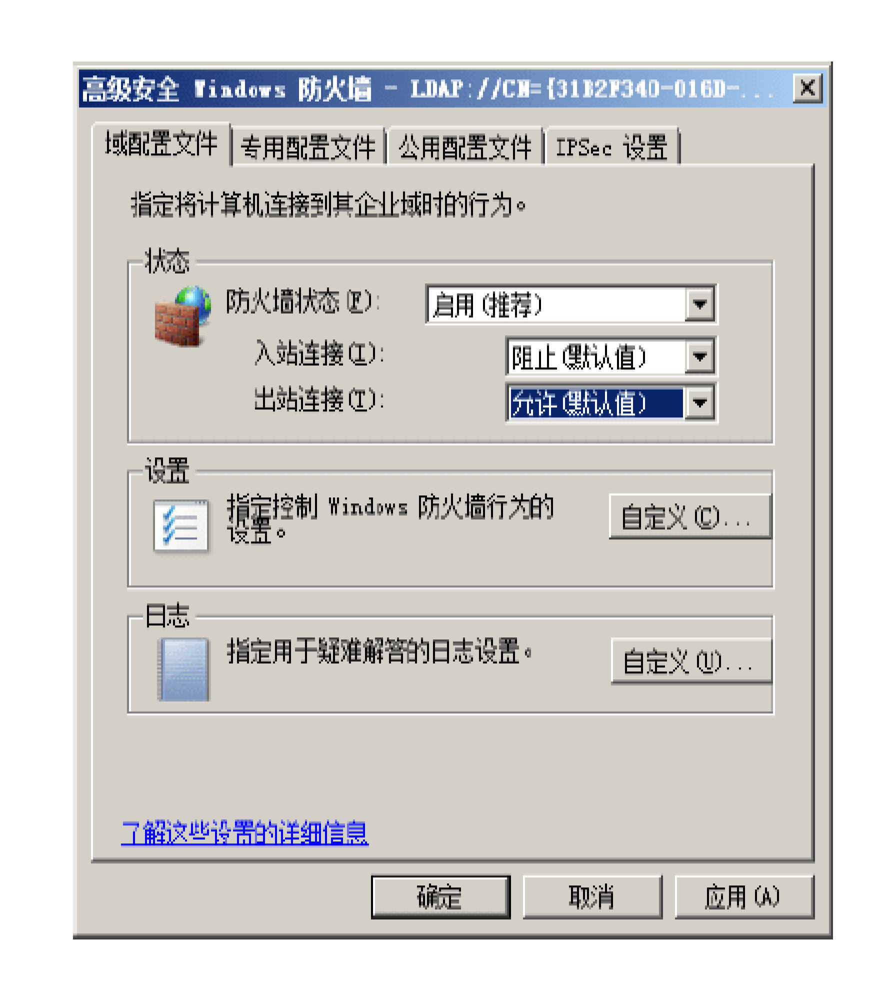


图 16.31　“高级安全 Windows 防火墙-LDAP 属性”对话框

注意　“专用配置文件”和“公用配置文件”选项卡中的设置，与“域配置文件”相同，此处不复赘述。

03 在“高级安全 Windows 防火墙-LDAP”中，右击“连接安全规则”并在快捷菜单中选择“新规则”选项。显示“规则类型”对话框，选择“隔离”单选按钮。单击“下一步”按钮，显示如图 16.32 所示“要求”对话框，选择“入站和出站连接请求身份验证”单选按钮。



图 16.32　打开“要求”对话框

04 单击“下一步”按钮，显示如图 16.33 所示“身份验证方法”对话框。选择“计算机证书”单选按钮，然后单击“浏览”按钮，查看并选择所使用的证书，并选中“只接受健康证书”复选框。





图 16.33 “身份验证方法”对话框

05 依次单击“下一步”按钮，设置配置文件类型和名称，如图 16.34 所示。在“配置文件”对话框中，选中“域”、“专有”和“公用”复选框。在“名称”对话框，设置防火墙规则名称和描述信息。

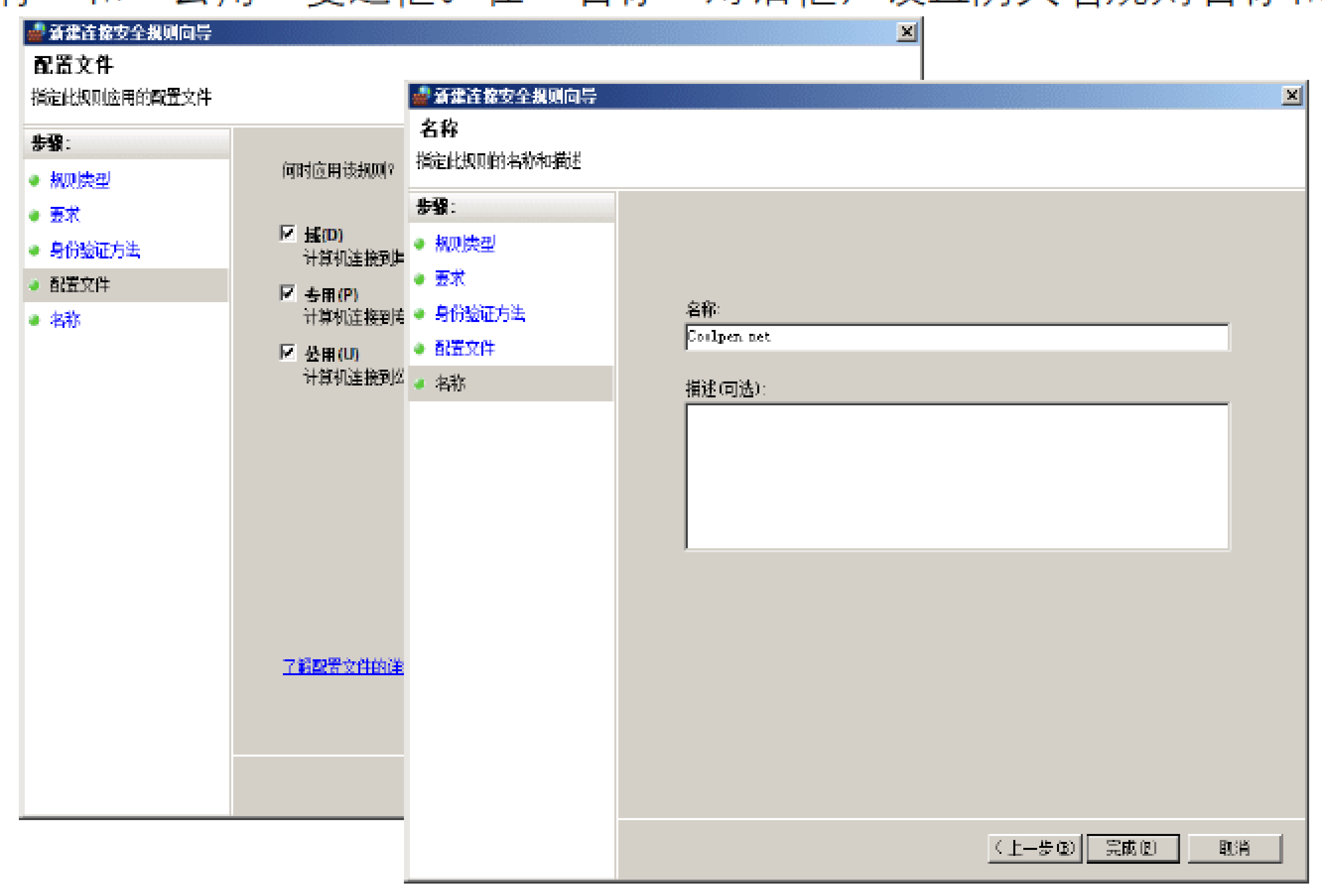


图 16.34 配置文件类型和规则名称

06 单击“完成”按钮，完成新规则的配置。

在创建完边界网络 GPO 后，需要将其应用于边界网络 OU 或安全组。在应用边界网络 GPO 到边界网络安全组或 OU 后，需要完成如下工作：

- 确保边界网络中的更新服务器能够收到边界网络 GPO 设置，并且拥有为入站和出站通讯请求 IPSec 保护的连接安全规则；
- 如果更新服务器可以收到边界网络 GPO 的设置，确保更新服务器可以建立与 NAP 客户端和非域成员计算机的通信，并且 NAP 客户端和非域成员计算机可以建立与更新服务器的通信。

在该阶段的 NAP 客户端、非域成员计算机和更新服务器之间的通信应该清除文本。更新服务器上的 IPSec 策略将会尝试越过 IPSec 保护，但是允许回退清除入站和出站通信尝试。

16.5　配置 DHCP 强制

DHCP 服务器是企业网络中的必备角色，其功能就是为入网用户分配当前局域网中的 IP 地址，使其可以访问网络中的资源。DHCP 强制需要在 DHCP 服务器上启用 NAP 功能，在分配 IP 之前，需对客户端健康进行评估。如果达到要求则允许访问所有网络资源，否则，为其分配仅应用于修补网络的 IP 地址，直到达到健康标准。

16.5.1　修改 DHCP 相关选项

当 DHCP 服务器被配置为 NPS 服务器时原有的 DHCP 服务器将被新的包含 NPS 功能的组件所取代，管理员需对 NPS 服务器涉及的 DHCP 选项进行重新配置。

1. 配置作用域

NPS 安装完成后，在 DHCP 作用域属性中，添加了一项“网络访问保护”选项卡，默认情况下，该设置没有被启用，需要管理员启用该设置。

01 选择“开始”→“管理工具”→“DHCP”命令，打开“DHCP 控制台”窗口。依次选择“win-91e1qh63qh63szj.corp.contoso.com”→“IPv4”选项，打开当前 DHCP 上的所有作用域。右击想要配置网络安全防护的作用域，在弹出的快捷菜单中选择“属性”命令，显示如图 16.35 所示“作用域[192.168.30.0] company 属性”对话框。

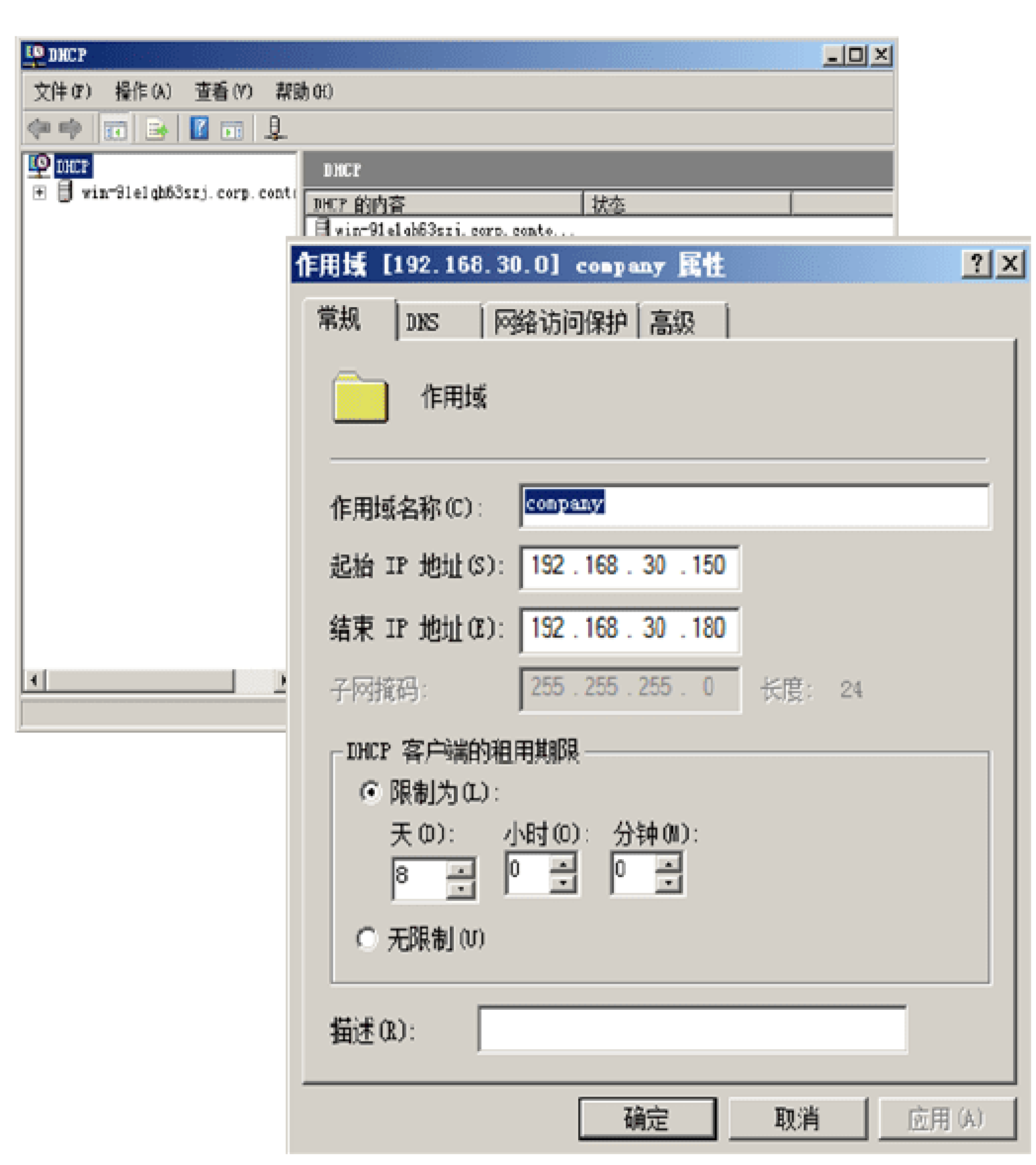


图 16.35　打开“作用域[192.168.30.0] company 属性”对话框

02 切换至“网络访问保护”选项卡，在“网络访问保护设置”选项框中，选中“对此作用域启用”单选按钮，如图 16.36 所示。



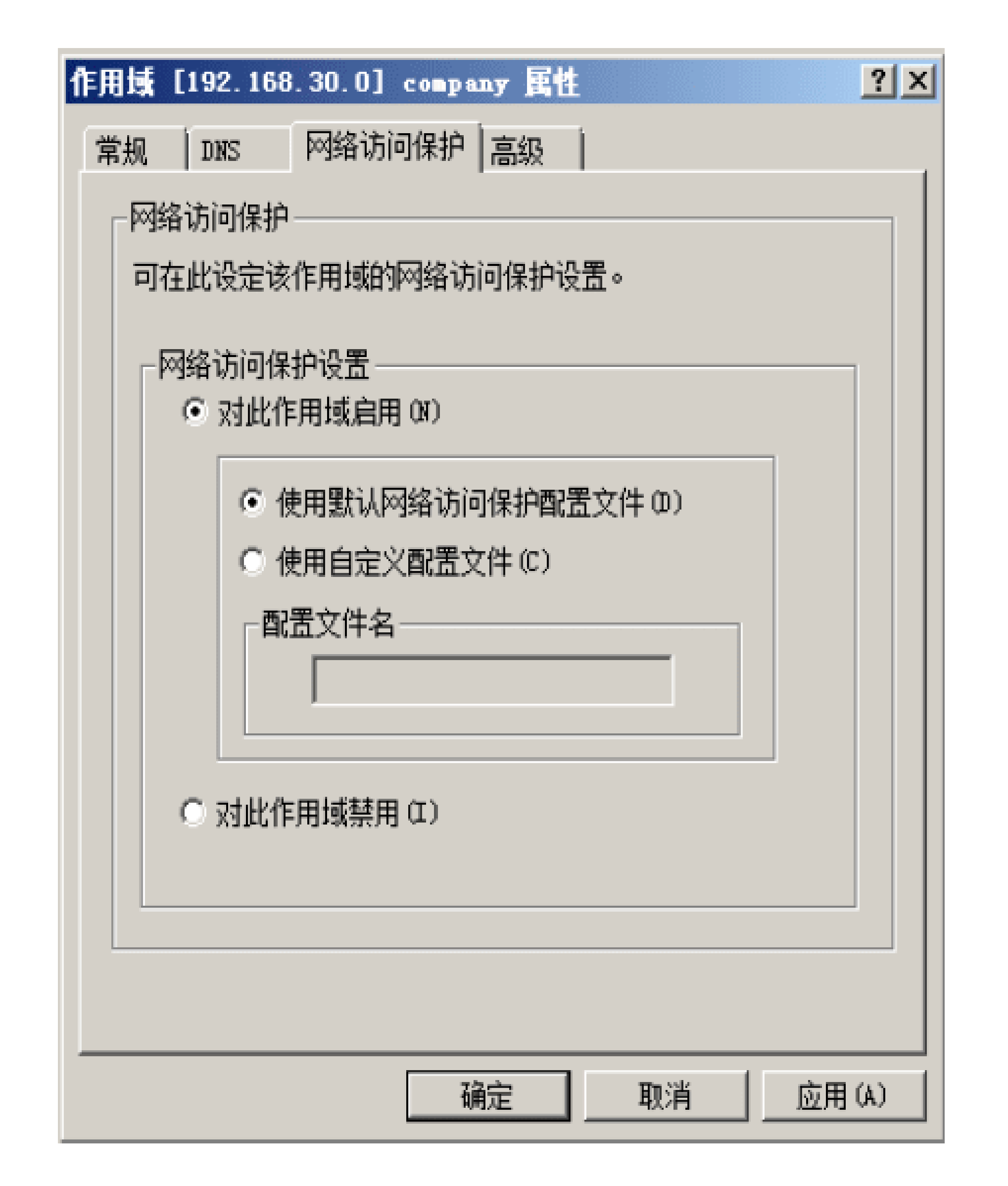


图 16.36　“网络访问保护”选项卡

03 单击“确定”按钮，保存设置并退出。

> 提示　Windows Server 2008 服务器同时提供 IPv6 下的 DHCP 服务，则还需要在 IPv6 的所有作用域中，执行相同操作。

2. 配置服务器选项

设置服务器选项，在为状态不良的客户端计算机提供租约时，会使用这组特殊的作用域选项（DNS 服务器、DNS 域名、路由器等）。例如提供给状态良好的客户端的默认 DNS 后缀为“company.com”，而提供给状态不良的客户端的 DNS 后缀为“Testcoolpen.com”。

01 在“DHCP”管理窗口中，选择“DHCP”→“WIN-91E1QH63SZJ.corp.contoso.com（服务器名）”→“IPv4”→“服务器选项”选项，右击“服务器选项”选项，在弹出的快捷菜单中的选择“配置选项”命令，显示如图 16.37 所示“服务器选项”对话框。

02 切换至“高级”选项卡，在“供应商类别”下拉列表中，选择“DHCP 标准选项”选项；在“用户类别”下拉列表中，选择“默认的网络访问保护级别”选项，如图 16.38 所示。

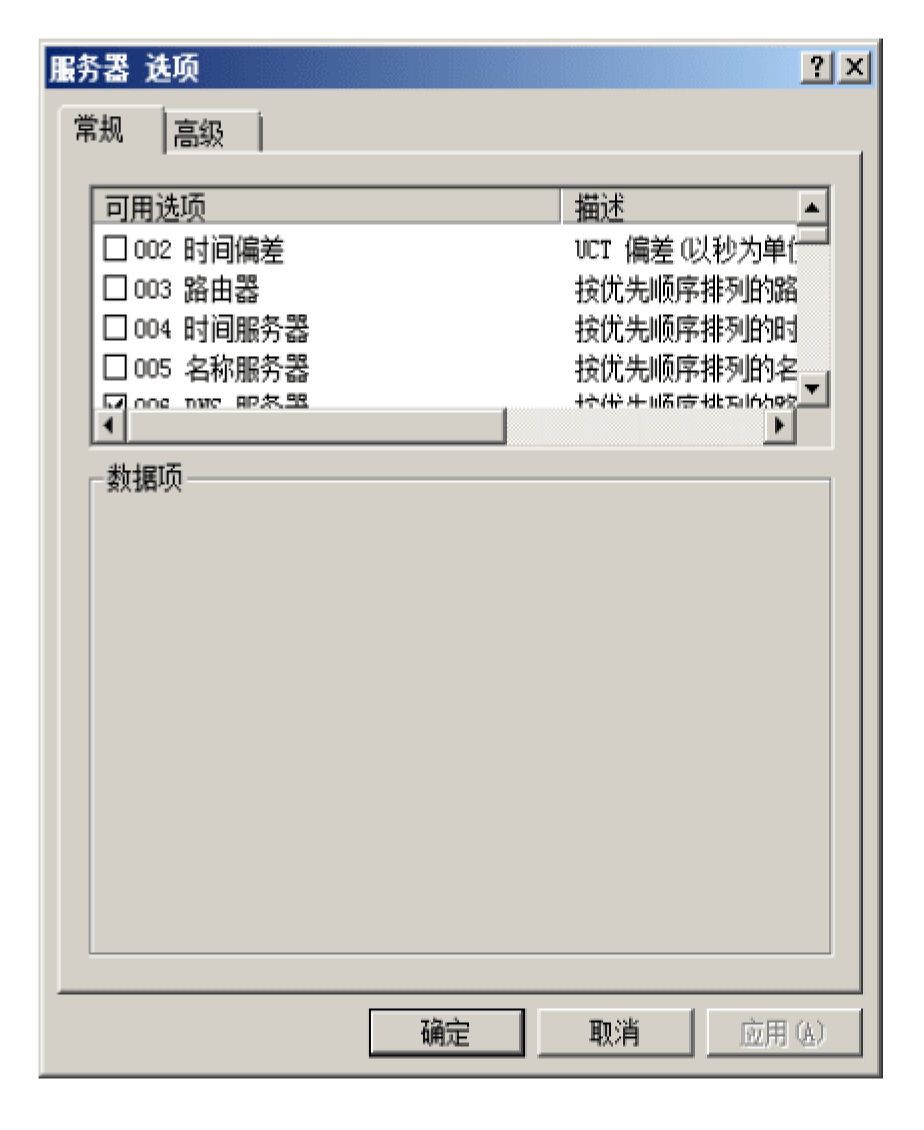


图 16.37 “服务器选项”对话框

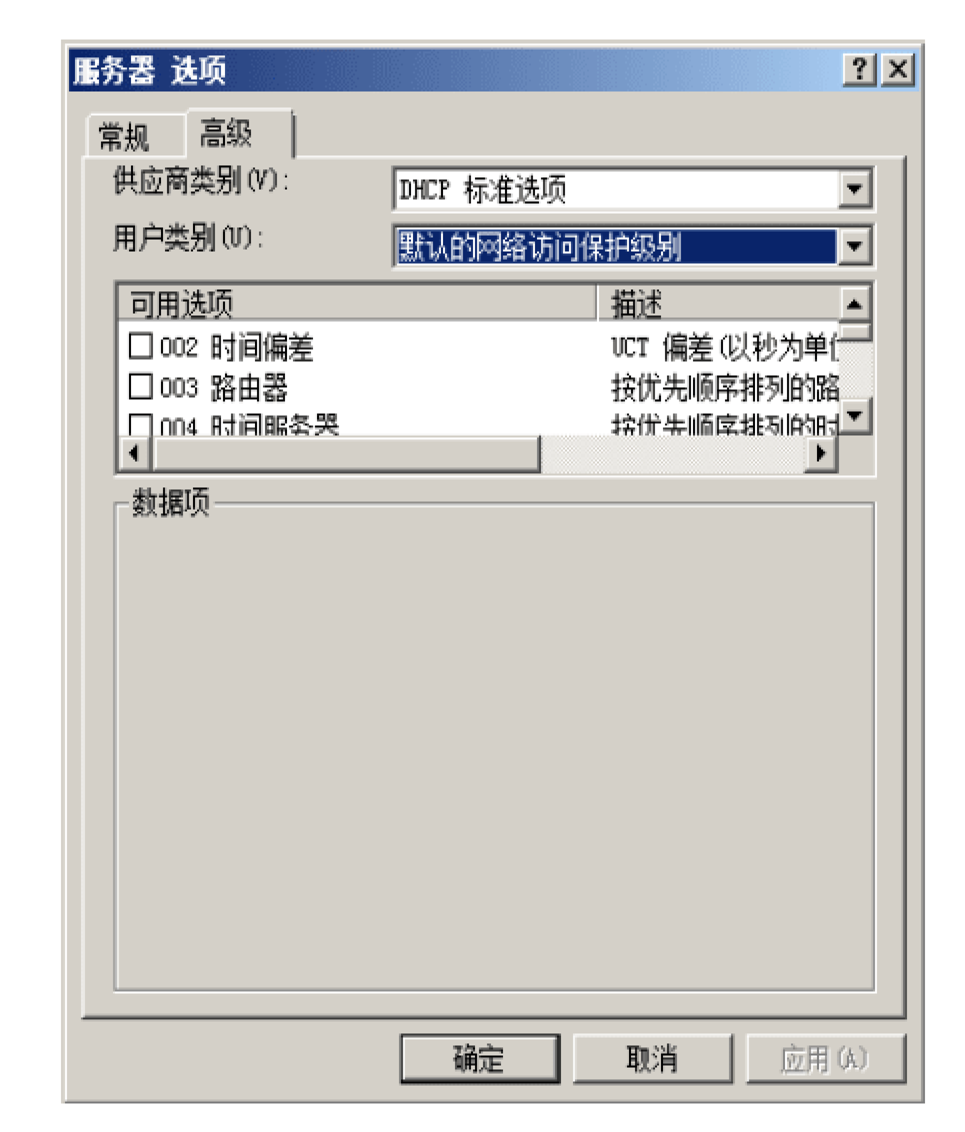


图 16.38 “高级”选项卡

03 在“可用选项”列表中，选中“003 路由器”复选框，在“IP 地址”文本框中，输入网络中路由器使用的 IP 地址，例如 192.168.2.3，单击“添加”按钮。如果网络中有多个路由器，可以再次添加。如果发现路由器的顺序错误，可以单击“下移”或者“上移”按钮，调整路由器的顺序，如图 16.39 所示。

04 在“可用选项”列表中，选择“006 DNS 服务器”复选框，在“IP 地址”文本框中，输入网络中 DNS 服务器使用的 IP 地址，单击“添加”按钮。如果网络中有多个 DNS，可以逐次添加。如果发现 DNS 服务器的顺序错误，可以单击“下移”或者“上移”按钮，调整 DNS 服务器的顺序，如图 16.40 所示。

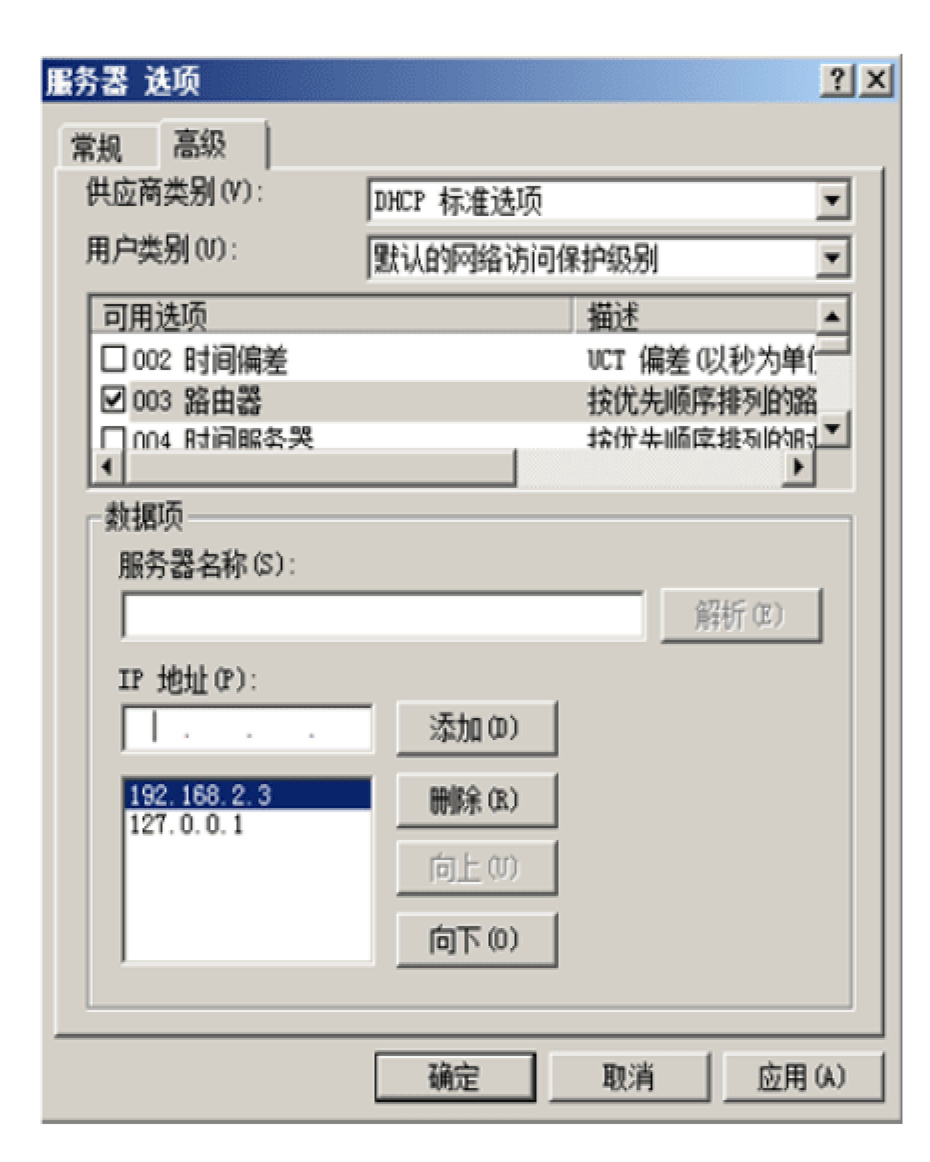


图 16.39 003 路由器

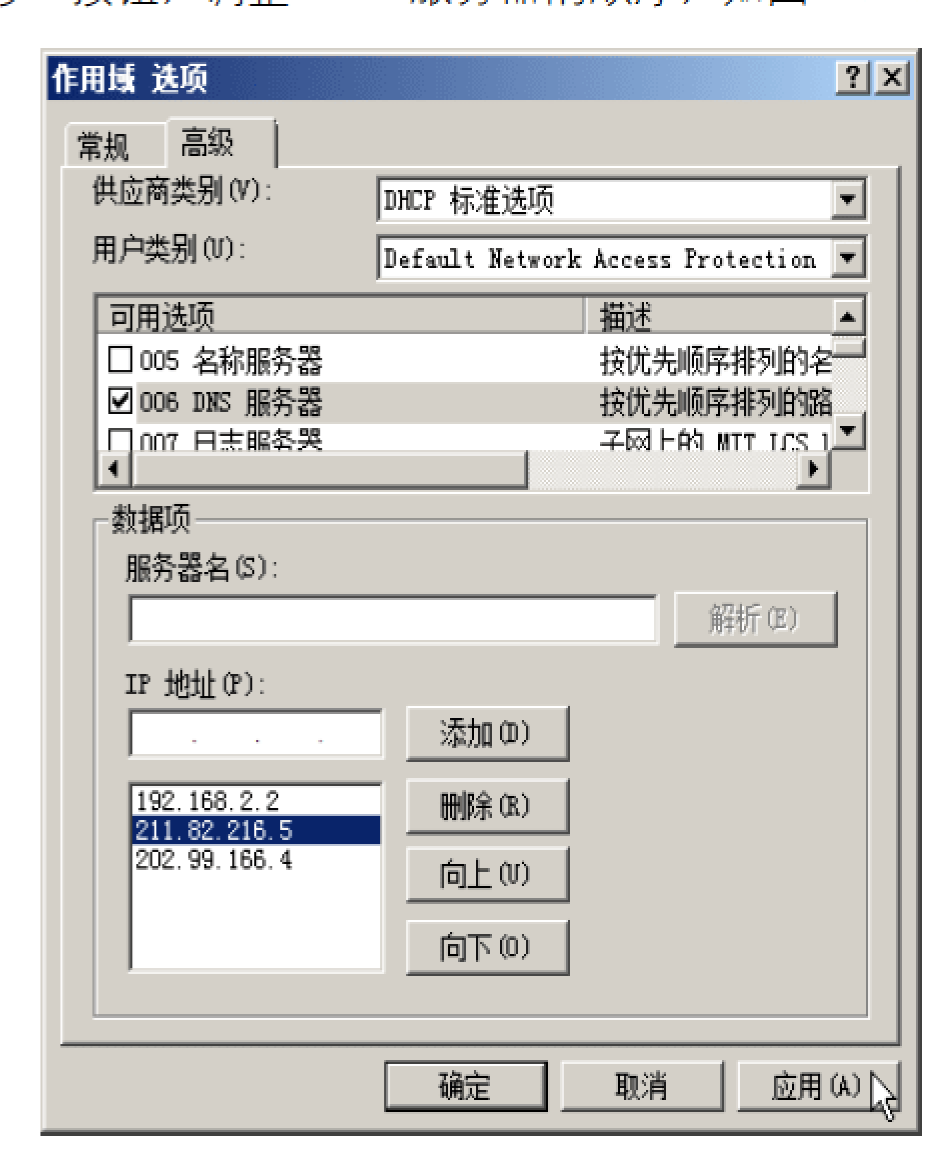


图 16.40 006 DNS 服务器

05 在“可用选项”列表中，选择“015 DNS 域名”复选框，在“数据项”选项框的“字符串值”文本框中，输入临时的 DNS 域名，如图 16.41 所示。



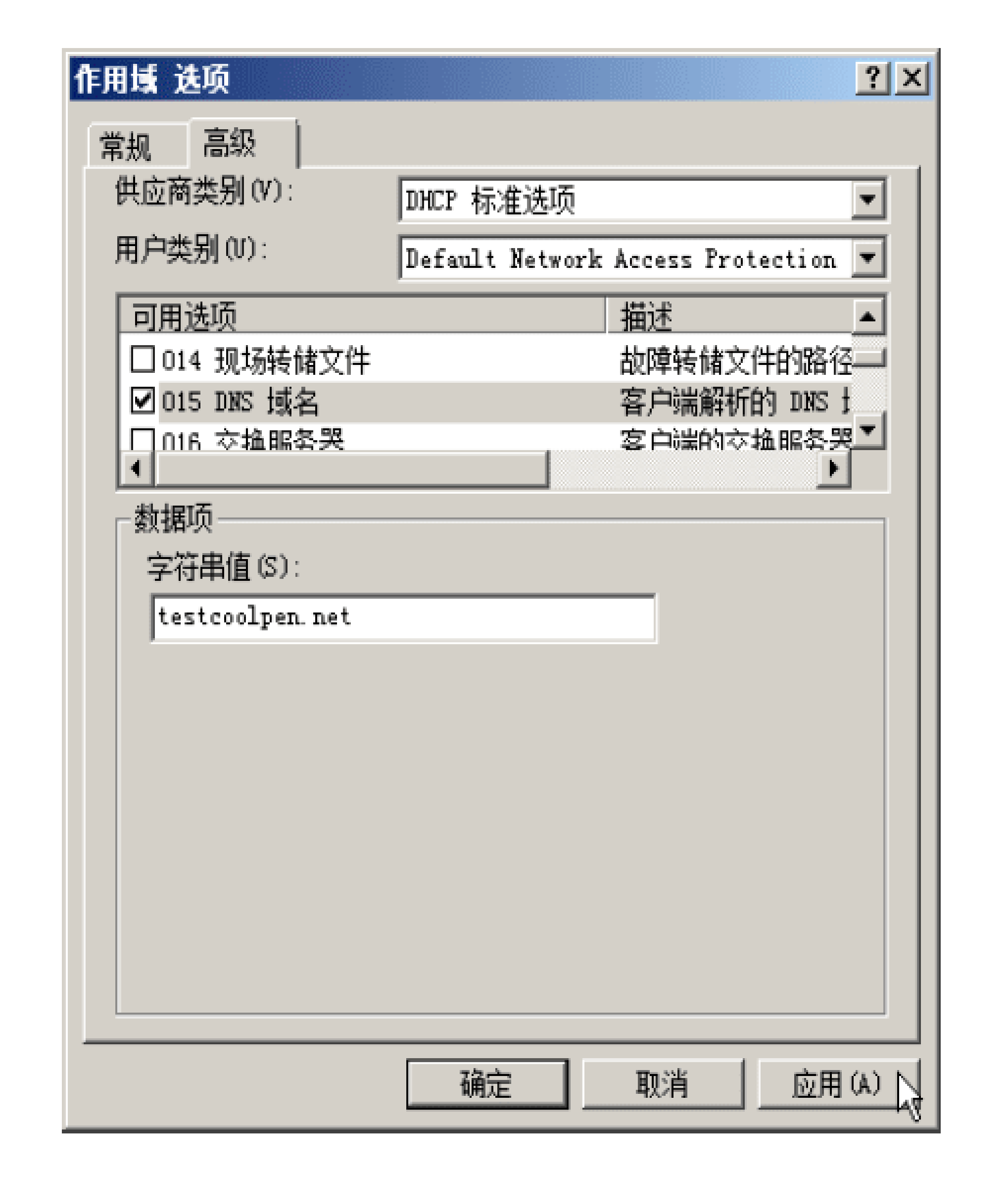


图 16.41　015 DNS 域名

06 单击“确定”按钮，完成服务器选项的设置。



提示　临时域的域名和 DHCP 安装过程创建的域名不同，没有实际的作用，只是方便网络管理员区分连到网络中的计算机，哪些是安全的，哪些是不安全的。例如如果计算机是安全的，则使用 company.com 域名；如果计算机不是安全的，使用这里指定的 Testcoolpen.com 域名。

16.5.2　配置 NPS 策略

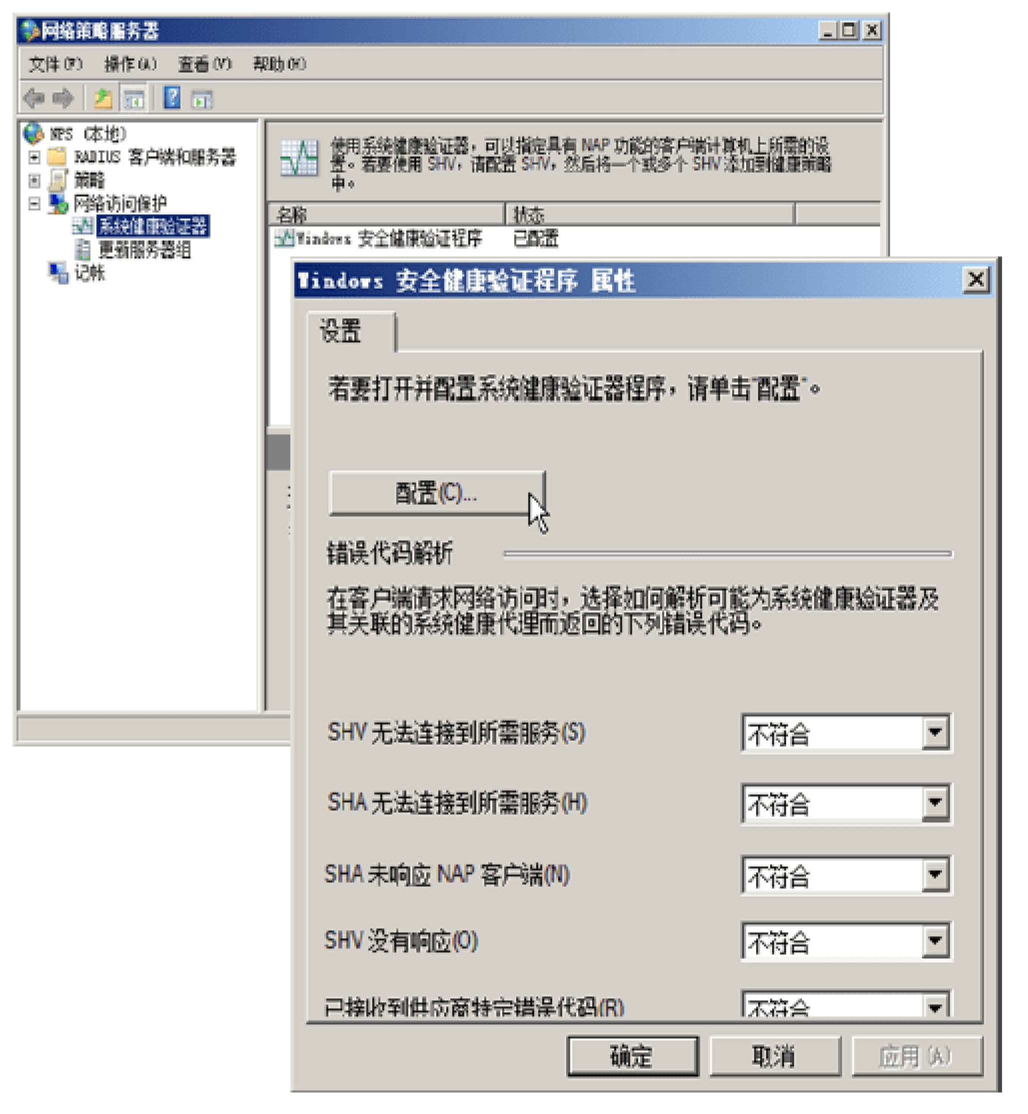
NPS 服务器由 4 个主要组件组成：网络健康验证器、更新服务器组、系统健康策略模板和网络策略。

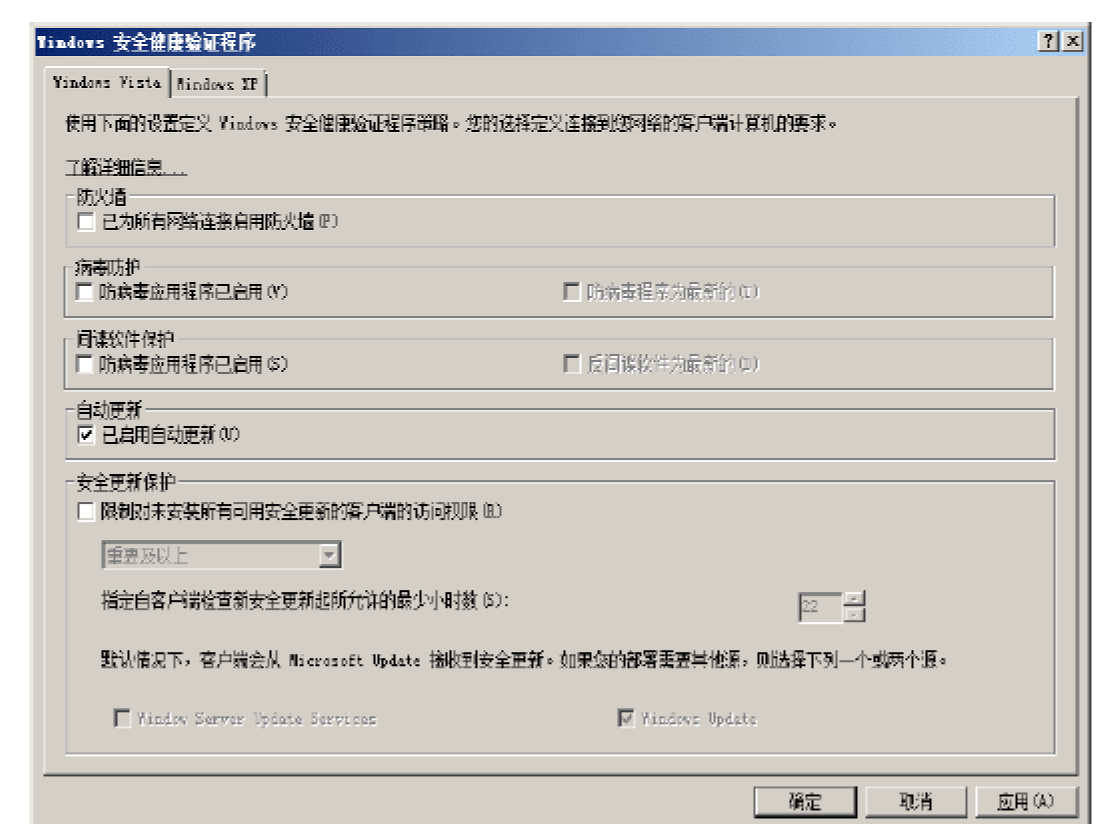
1. 设置网络健康验证器

通过网络健康验证器策略，可以检测连接到网络中的计算机是否安全，例如没有开启自动更新的计算机就认为不安全、没有安全防病毒软件就是不安全的计算机等。

01 选择“开始”→“管理工具”→“网络策略服务器”命令，打开“网络策略服务器”窗口。选择“NPS（本地）”→“网络访问保护”→“系统健康验证器”选项，右击“Windows 安全健康验证程序”选项，在弹出的快捷菜单中选择“属性”命令，打开如图 16.42 所示“Windows 安全健康验证程序 属性”对话框。

02 单击“配置”按钮，显示如图 16.43 所示“Windows 安全健康验证程序”对话框，选中需要健康检测内容的复选框。


图 16.42 “Windows 安全健康验证程序 属性”对话框


图 16.43 Windows 系统健康验证程序

03 单击“确定”按钮，保存配置。

2. 配置更新服务器组

配置更新服务器组可以使状态不良的计算机访问网络资源，包括 WSUS 或 SMS 服务器等。头盖骨访问定义的系统，使受限制的计算机恢复到正常状态。

01 在“网络策略服务器”窗口中，依次展开“NPS（本地）”→“网络访问保护”→“更新服务器组”选项。右击“更新服务器组”选项，选择快捷菜单中的“新建”命令，显示“新建更新服务器组”对话框。在“组名”文本框中，输入服务器组的名称，如 company。单击“添加”按钮，显示如图 16.44 所示“添加新服务器”对话框。在“友好名称”文本框中，输入目标服务器的标识名称。在“IP 地址或 DNS 名称”文本框中，输入当验证客户端验证不能通过时，需要到目标服务器进行处理或者暂时访问的目标服务器，可以使用 IP 地址或 DNS 名称。

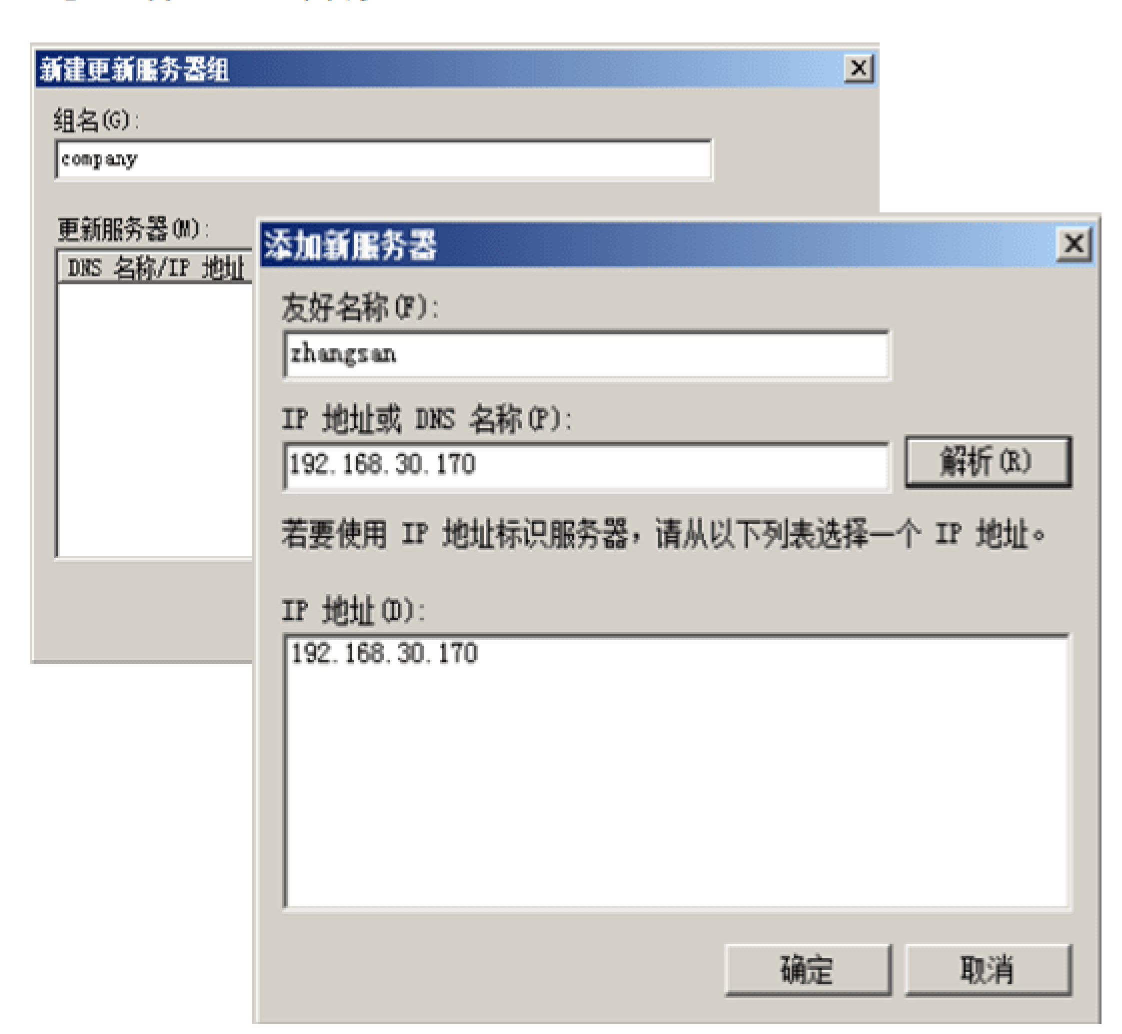


图 16.44 打开“添加新服务器”对话框



02 依次单击“确定”按钮，返回“网络策略服务器”窗口，即可看到成功创建的更新服务器组。

3. 配置系统健康策略模板

使用系统健康策略模板来评估客户端计算机是否健康，验证模板会获取 SHV 检查的结果，根据计算机是否通过其中的一项或多项检查，确定其运行状态是否良好。

01 在“网络策略服务器”窗口中，选择“NPS（本地）”→“策略”→“健康策略”选项，显示“健康策略”窗口。右击“健康策略”选项，在弹出的快捷菜单中选择“新建”命令，显示如图 16.45 所示“新建健康策略”对话框。在“策略名称”文本框中，输入健康策略的名称，如安全策略。在“客户端 SHV 检查”下拉列表中，选择“客户端通过了所有 SHV 检查”选项。在“此健康策略中使用的 SHV”列表中，选中“Windows 安全健康验证程序”复选框即可。

02 按照相同的操作，再创建一条判断计算机为不安全计算机的策略，如图 16.46 所示。根据实际需要，在“客户端 SHV 检查”下拉列表中选择相应级别的标准，如“客户端未能通过一个或多个 SHV 检查”等。

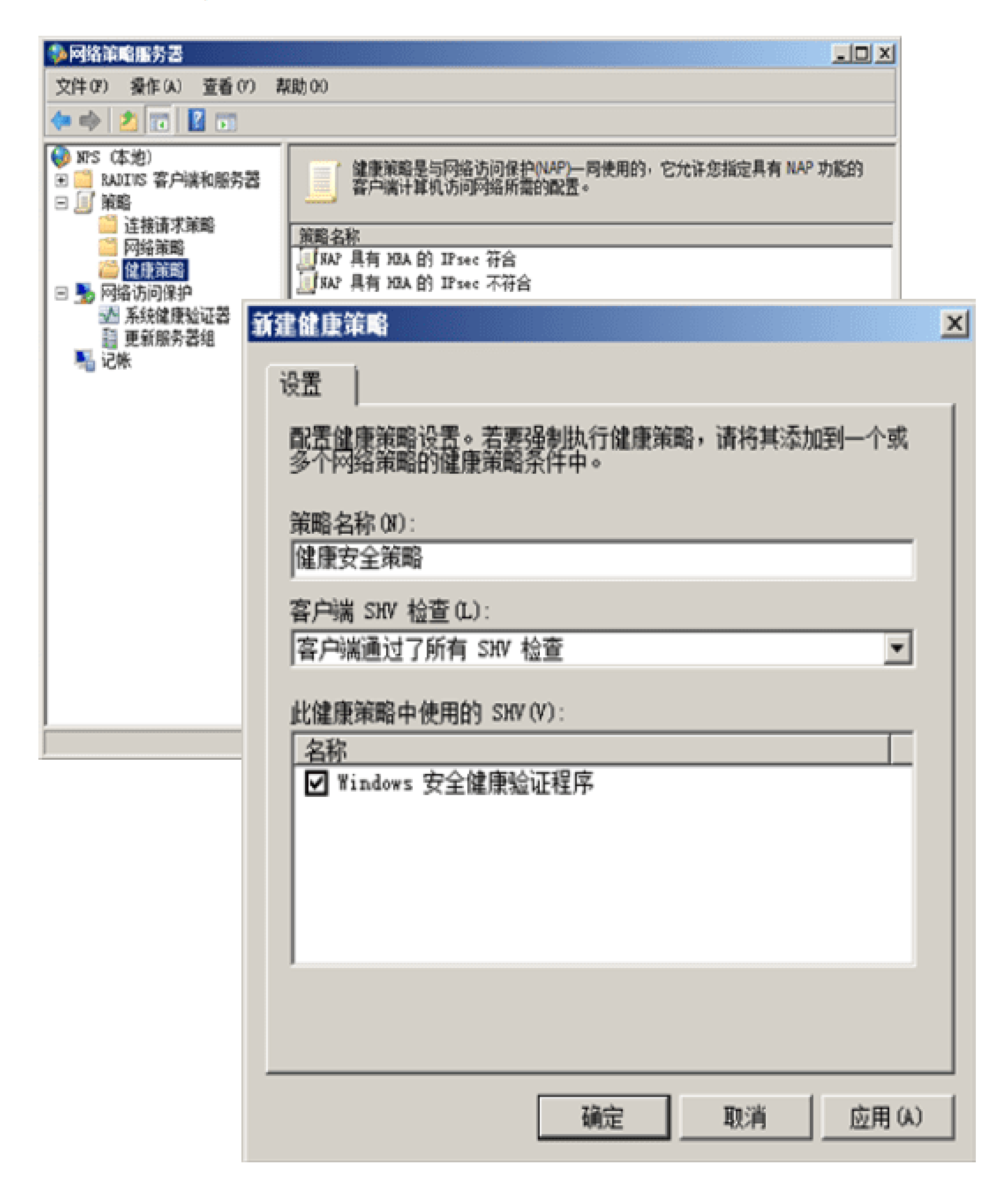


图 16.45 打开“新建健康策略”对话框

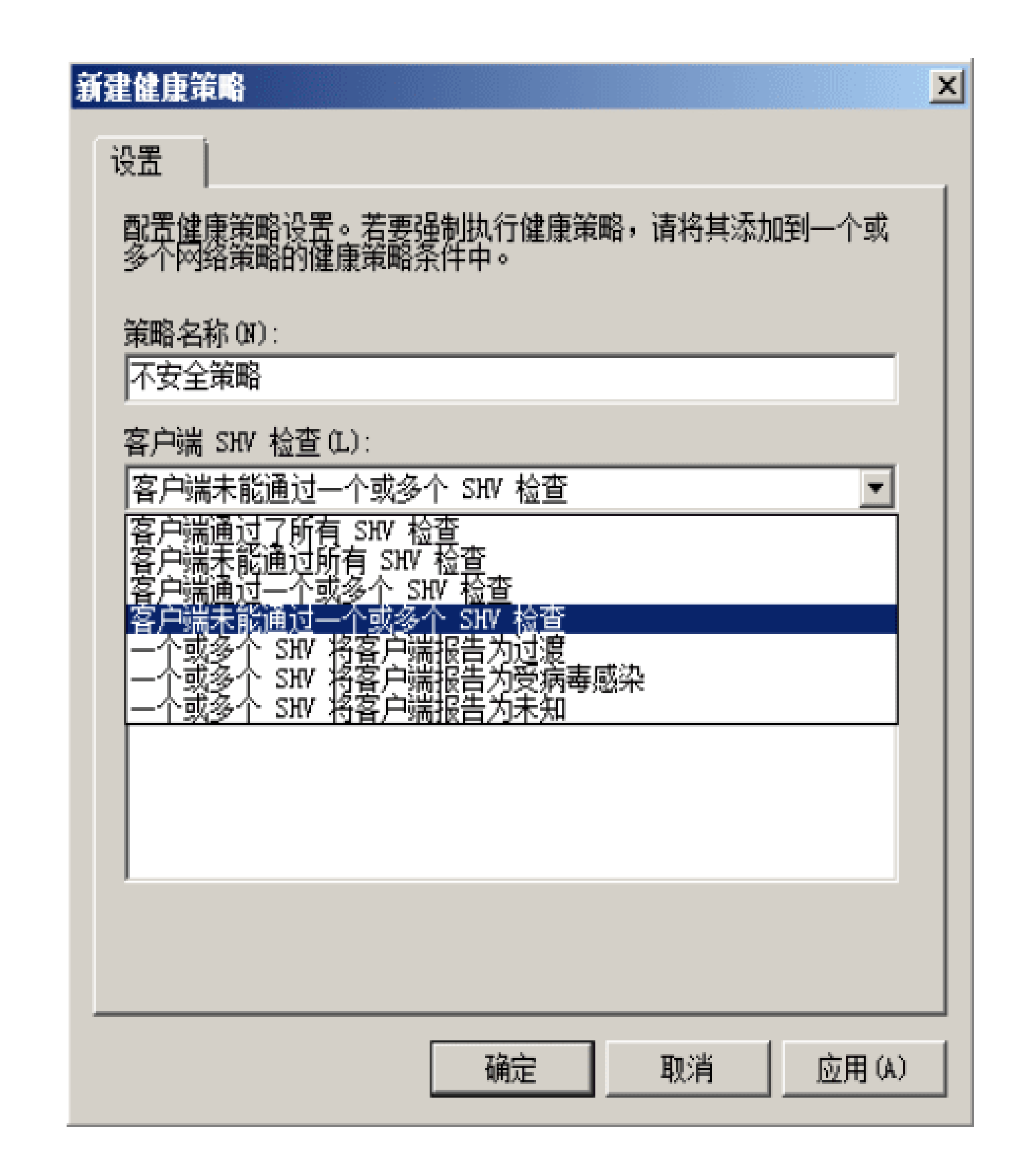


图 16.46 创建不安全策略

03 单击“确定”按钮，关闭“新建健康策略”对话框。已经创建的“安全策略”和“不安全策略”即可显示在“健康策略”列表中。

4. 配置网络策略

管理员定义网络策略，根据计算机运行状况确定如何对其进行处理。NPS 会从上到下执行启用的所有策略。在配置健康策略模板时，创建了“安全策略”和“不安全策略”，接下来将这两条健康策略应用到实际网络环境中。

01 在“网络策略服务器”窗口中，选择“NPS（本地）”→“策略”→“网络策略”选项，右击“网络策略”选项，在弹出的快捷菜单中的选择“新建”命令，显示如图 16.47 所示“指定网络策略名称和连接

类型”对话框。在“策略名称”文本框中输入合适的名称，选择“网络访问服务器类型”单选按钮，在下拉列表中选择“DHCP 服务器”选项。

02 单击“下一步”按钮，显示“指定条件”对话框，继续单击“添加”按钮，显示如图 16.48 所示“指定条件”对话框，在条件列表中选择“健康策略”，即可使用已经创建的健康策略。

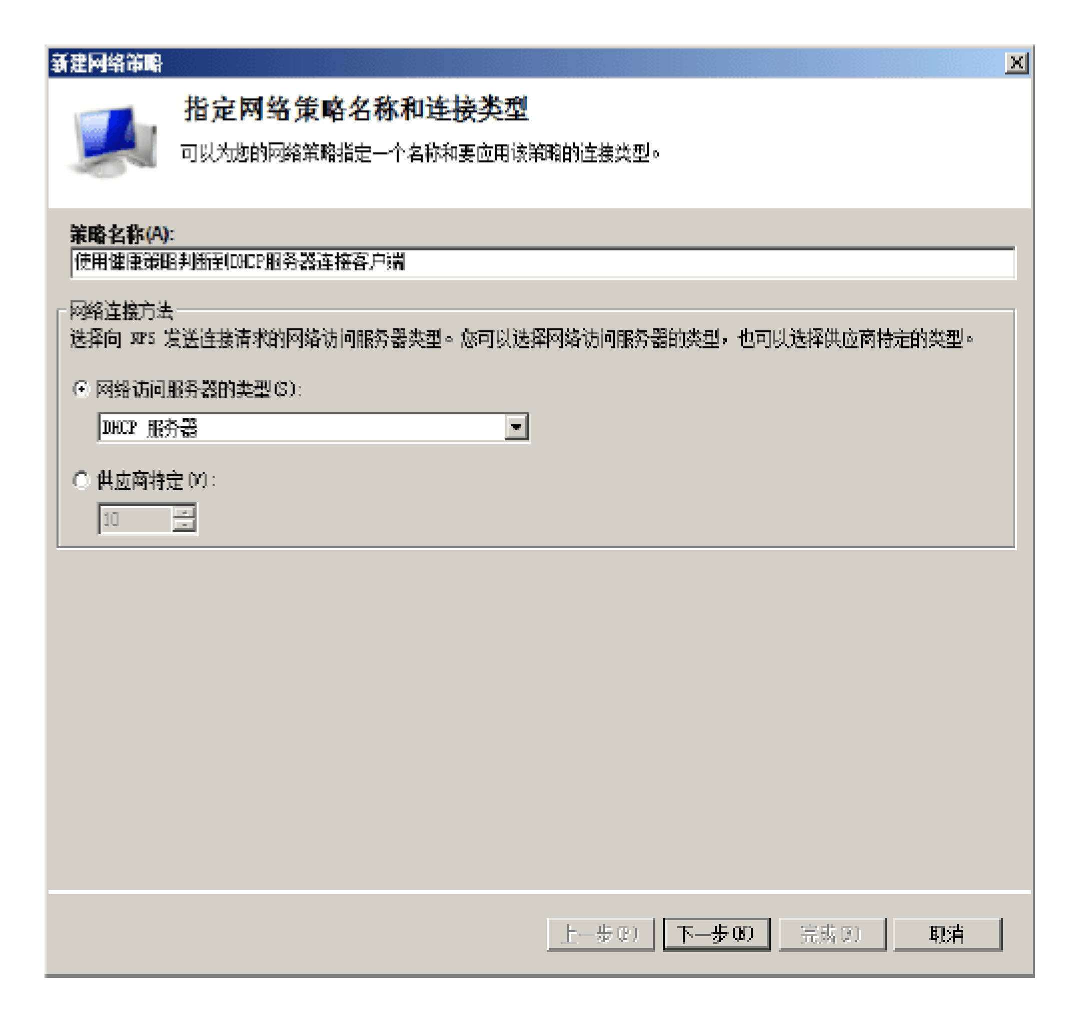


图 16.47 “指定网络策略名称和连接类型”对话框

图 16.48 “指定条件”对话框

03 单击“添加”按钮，显示如图 16.49 所示“健康策略”对话框，在“健康策略”下拉列表中，选择想要应用的策略即可。单击“确定”按钮，添加到“指定条件”对话框中。再次执行相同的操作，还可以添加其他策略或条件。

04 依次单击“下一步”按钮，设置访问权限和身份验证方法，如图 16.50 所示。在“指定访问权限”对话框中，如果符合条件中健康策略的判定标准，要授予网络访问权限还是要拒绝网络访问。这里选中“已授予访问权限”单选按钮，即通过健康策略验证的客户端均可正常访问 DHCP 服务器。在“配置身份验证方法”对话框中，本例使用 Windows 系统健康程序对客户端计算机进行验证，因此只选中“仅执行计算机健康检查”复选框即可。

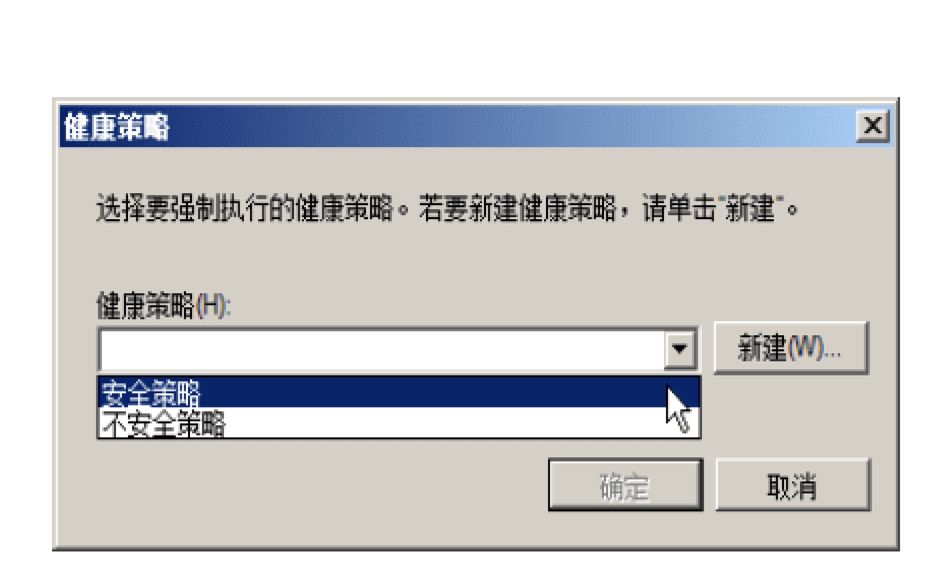


图 16.49 “健康策略”对话框

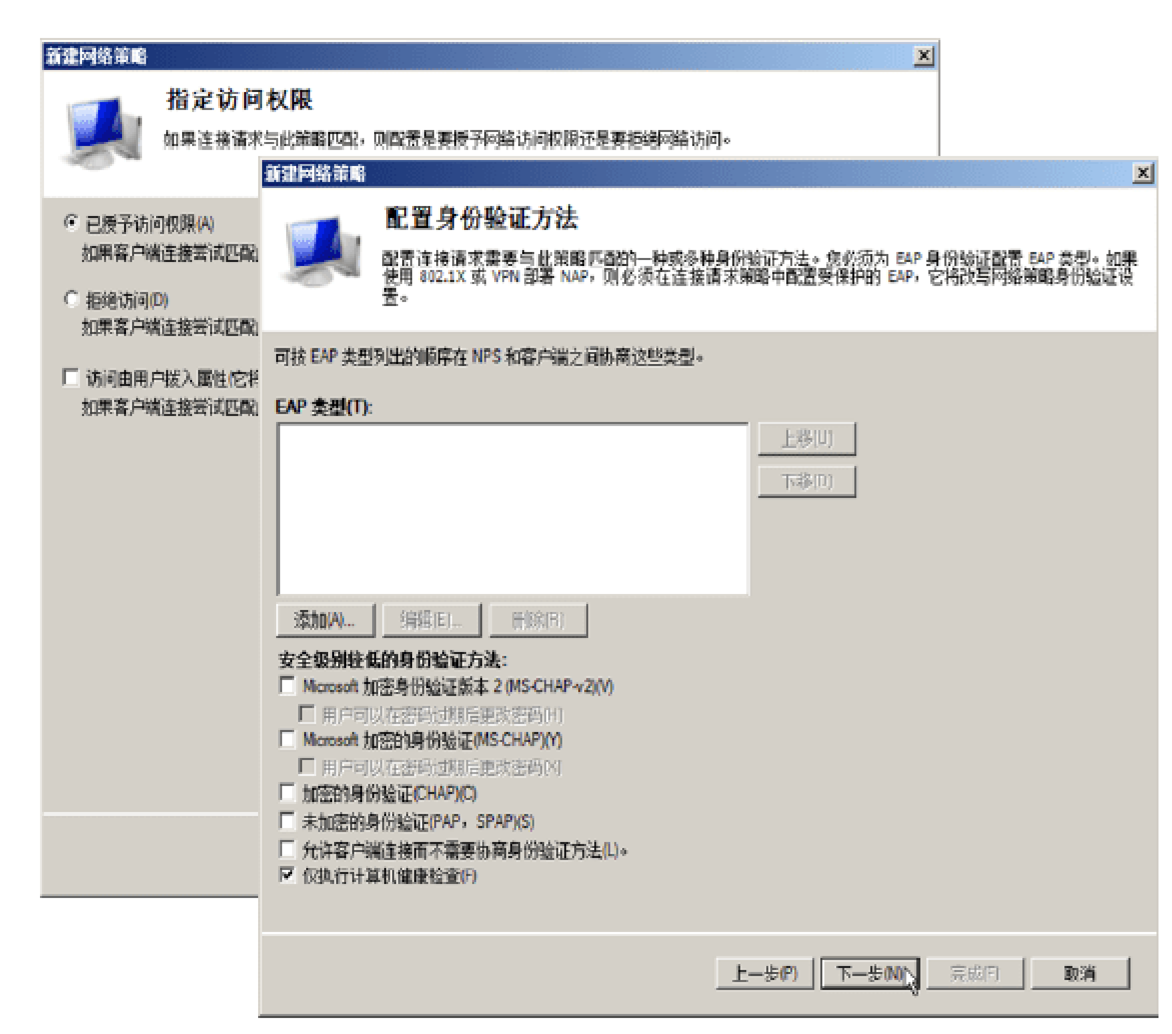


图 16.50 指定访问权限和身份验证方法



05 依次单击“下一步”按钮，设置约束条件和其他选项，如图 16.51 所示。在“配置约束”对话框中，进行进一步设置，包括连接超时限制等。在“配置设置”对话框中，根据实际需要进行相关设置即可，也可以使用默认设置。

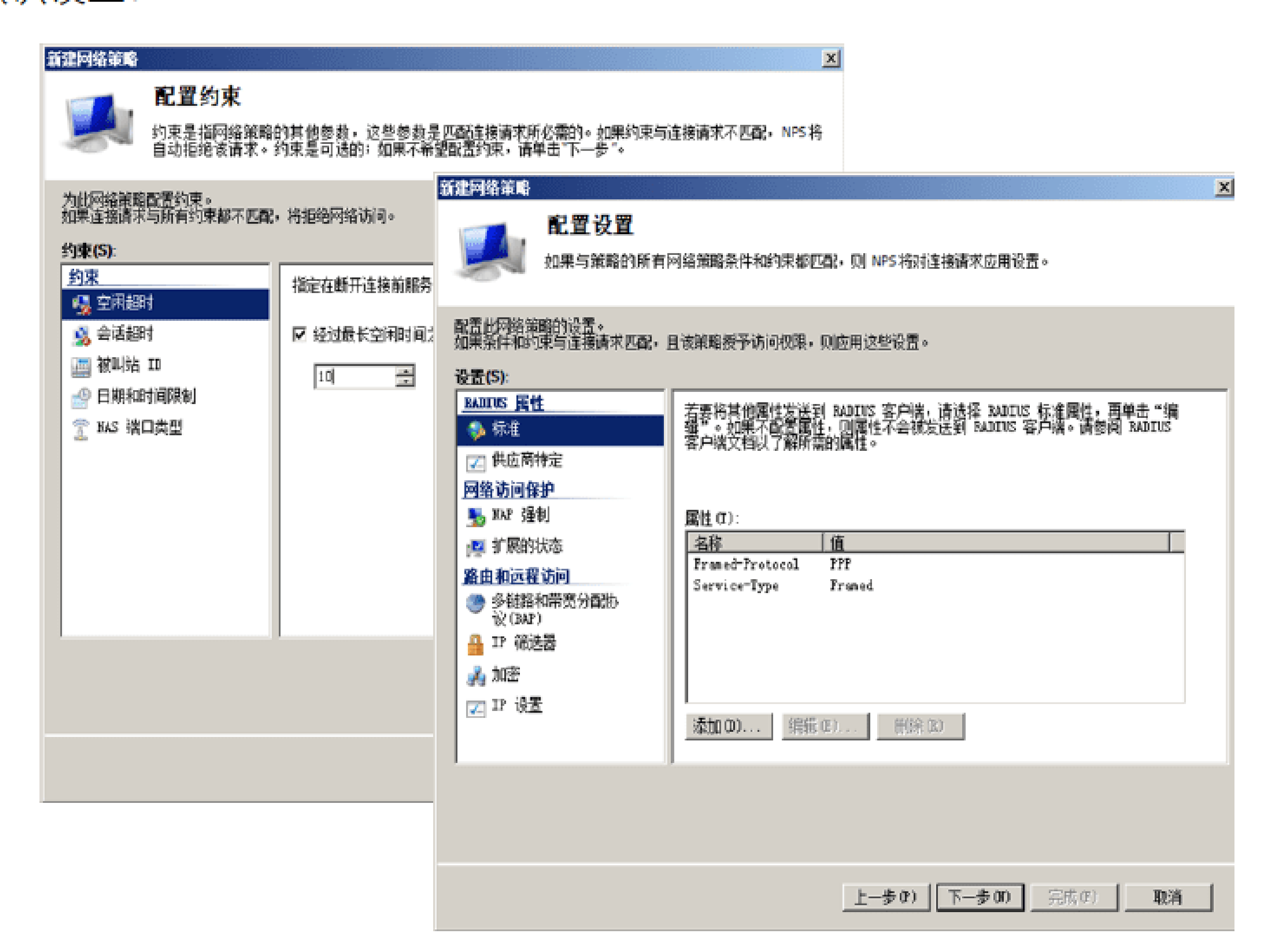


图 16.51　设置约束条件和其他选项

06 单击“下一步”按钮，显示“正在完成新建网络策略”对话框，单击“完成”按钮，返回“网络策略服务器”窗口，如图 16.52 所示。

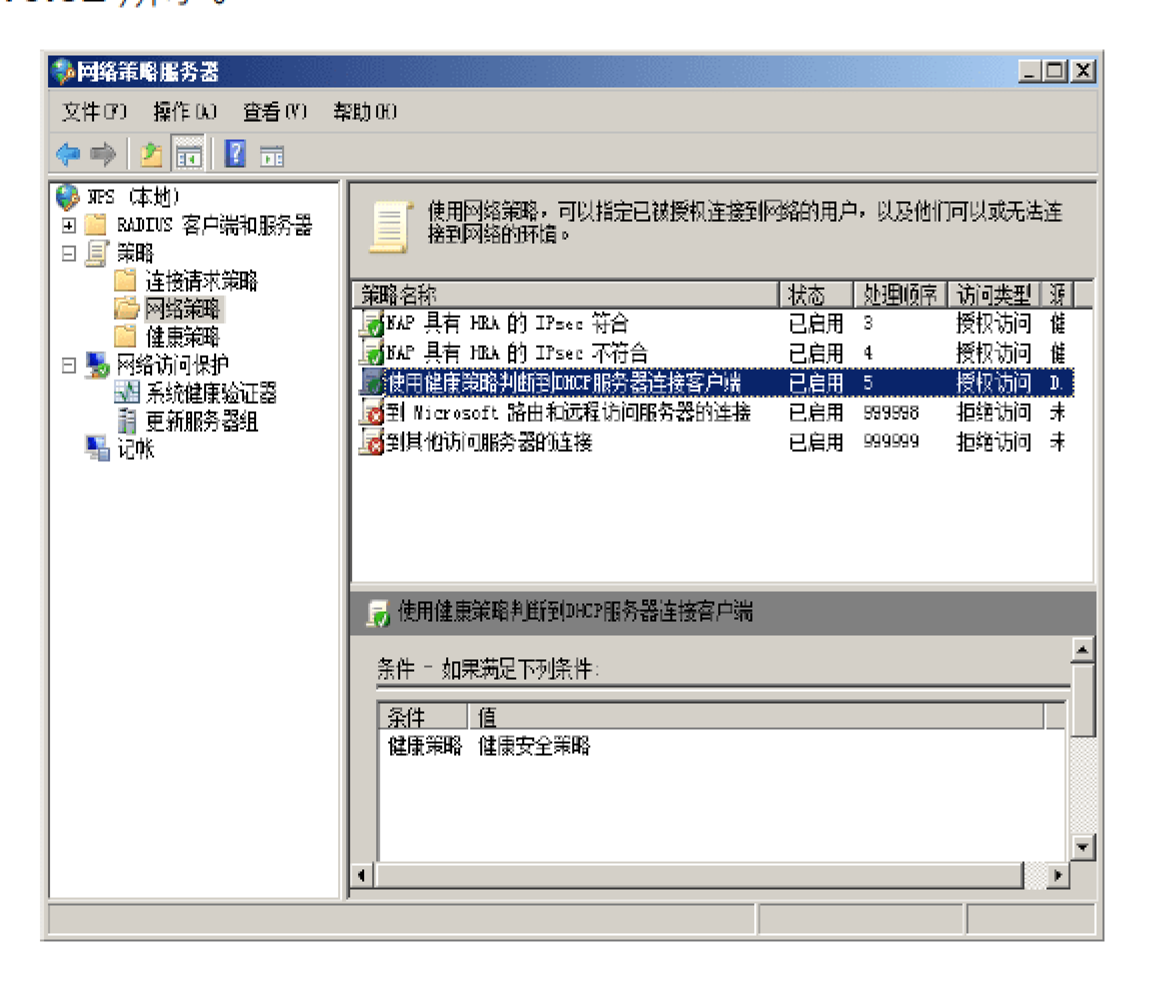


图 16.52　将健康策略应用到网络策略中

按照上述配置，符合“安全策略”验证要求的客户端，可以享有正常的访问权限，但并不会对不符合要求的客户端进行任何修复或整理操作，因此还需要将“不安全策略”应用到网络策略中。操作方法与前面完全相同。但当运行至如图 16.53 所示“配置设置”步骤时，选择“网络访问保护”选项中的“NAP 强制”选项，在右侧窗格中选中“允许受限访问”单选按钮。

单击“配置”按钮，显示如图 16.54 所示“更新服务器和疑难解答 URL”对话框。在“更新服务器组”下拉列表项中，选择此类型受限客户端允许访问的服务器组。“疑难解答 URL”是方便来访用户了解网络访问策略要求的公告性网页或文本，用户可根据需要自定义。



图 16.53 “配置设置”对话框

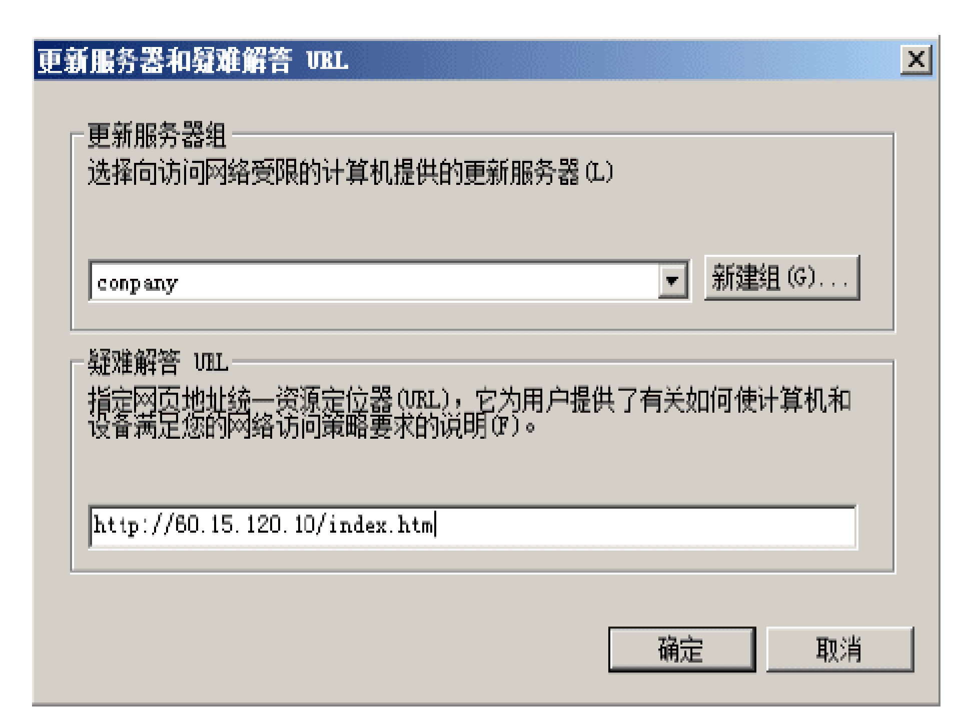


图 16.54 “更新服务器和疑难解答 URL”对话框

16.5.3 配置 DHCP 强制客户端

DHCP 强制客户端的配置过程与 IPSec 强制客户端类似，不同的是，在配置 NAP 客户端代理组件时，应启用“DHCP 隔离强制客户端”选项，如图 16.55 所示。其他配置操作完全相同，此处不复赘述。

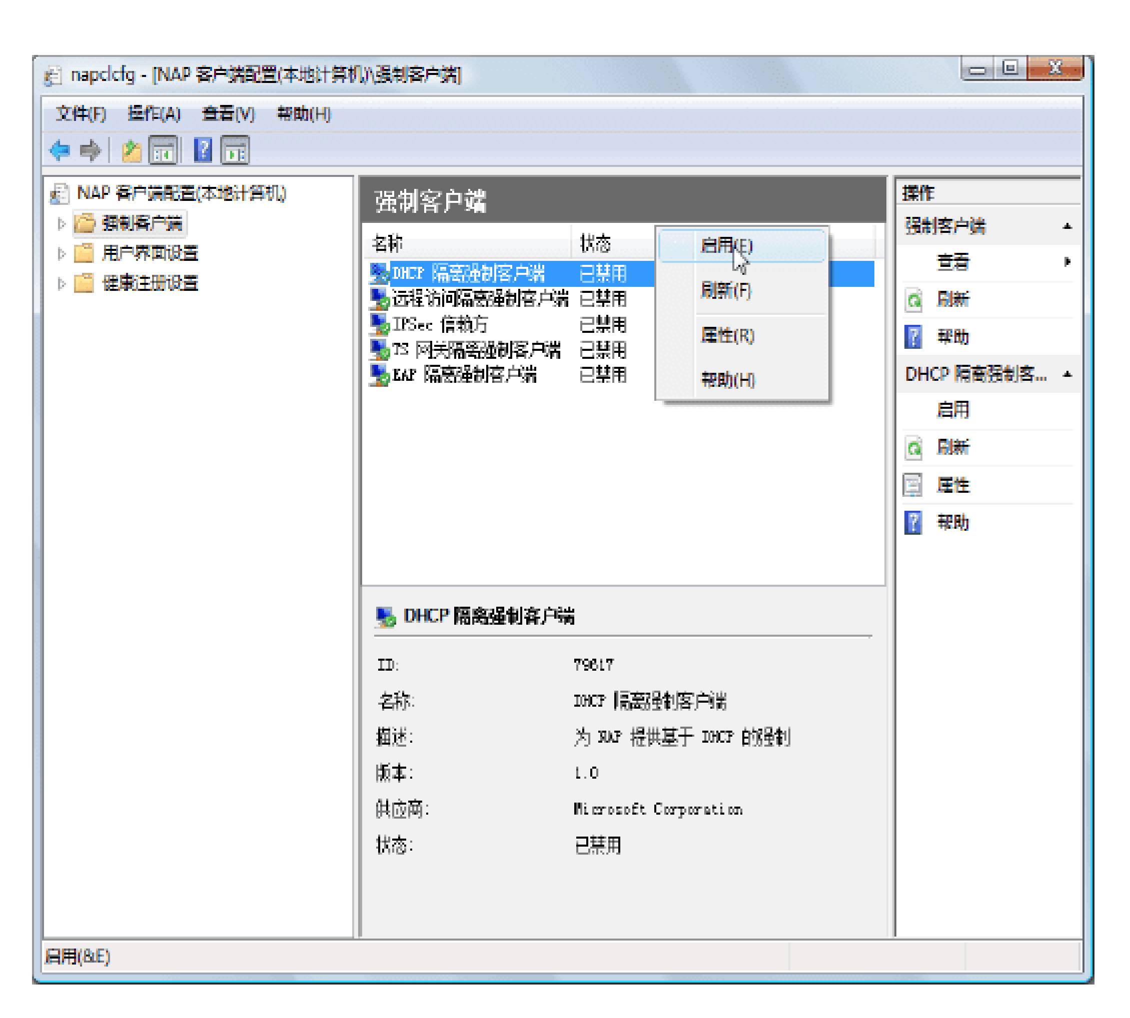


图 16.55 启用“DHCP 隔离强制客户端”

16.5.4 测试 DHCP 强制

如果客户端在没有开启系统防火墙或者没有开启自动更新的情况下，登录域控制器后，任务栏中会提示“此计算机不符合该网络策略的要求”。说明 NAP 服务器开始发挥作用了。此时该客户端不能继续访问网络中的某些服务器或计算机。单击提示信息，打开如图 16.56 所示“网络访问保护”对话框。该窗口中提示当前客户端未能通过网络策略检测的原因，并给出解



图 16.53 “配置设置”对话框

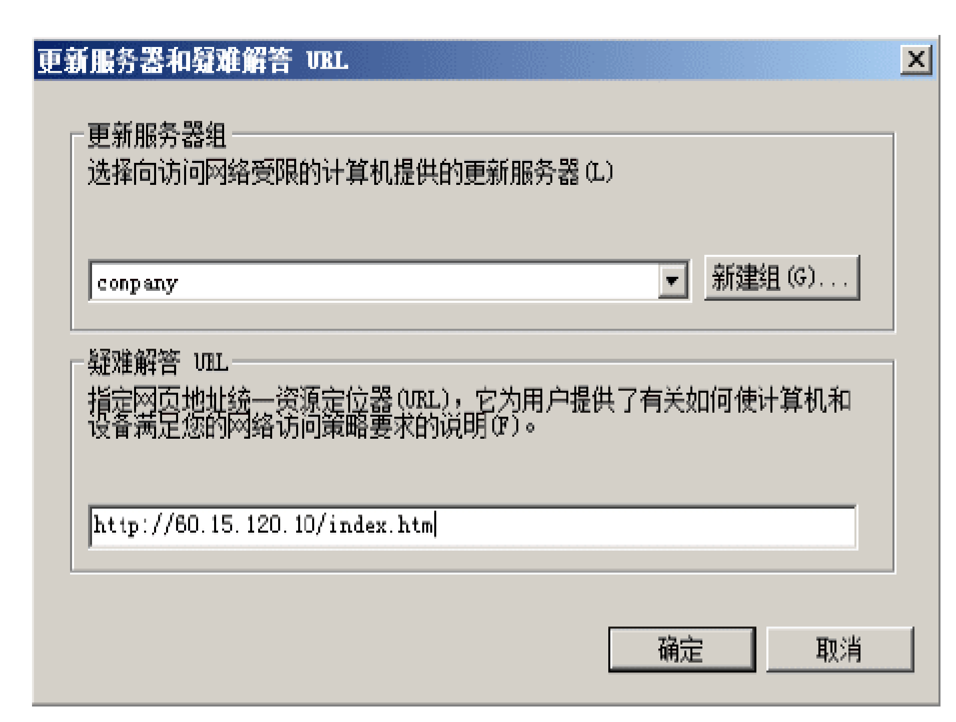


图 16.54 “更新服务器和疑难解答 URL”对话框

16.5.3 配置 DHCP 强制客户端

DHCP 强制客户端的配置过程与 IPSec 强制客户端类似，不同的是，在配置 NAP 客户端代理组件时，应启用“DHCP 隔离强制客户端”选项，如图 16.55 所示。其他配置操作完全相同，此处不复赘述。

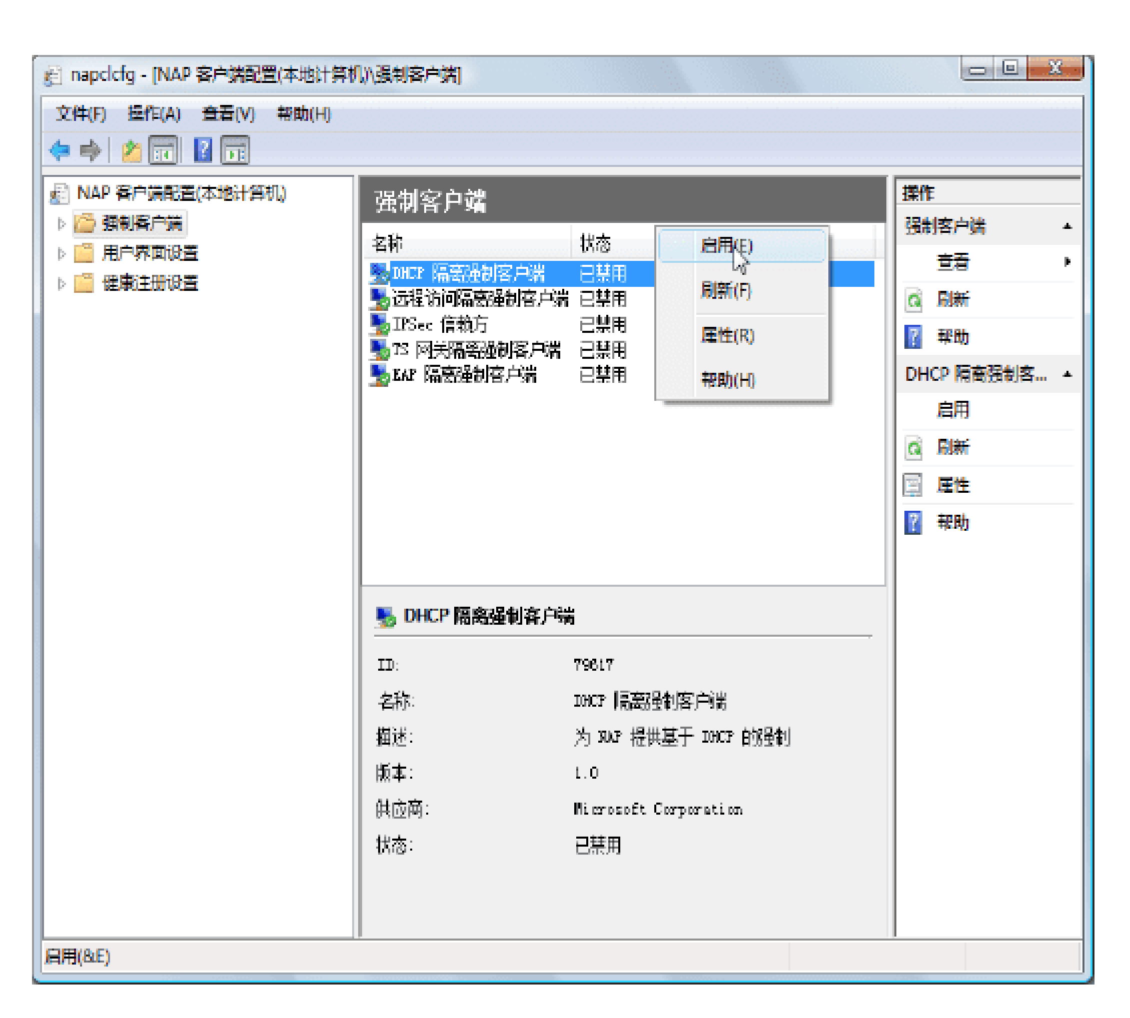


图 16.55 启用“DHCP 隔离强制客户端”

16.5.4 测试 DHCP 强制

如果客户端在没有开启系统防火墙或者没有开启自动更新的情况下，登录域控制器后，任务栏中会提示“此计算机不符合该网络策略的要求”。说明 NAP 服务器开始发挥作用了。此时该客户端不能继续访问网络中的某些服务器或计算机。单击提示信息，打开如图 16.56 所示“网络访问保护”对话框。该窗口中提示当前客户端未能通过网络策略检测的原因，并给出解



图 16.53 “配置设置”对话框

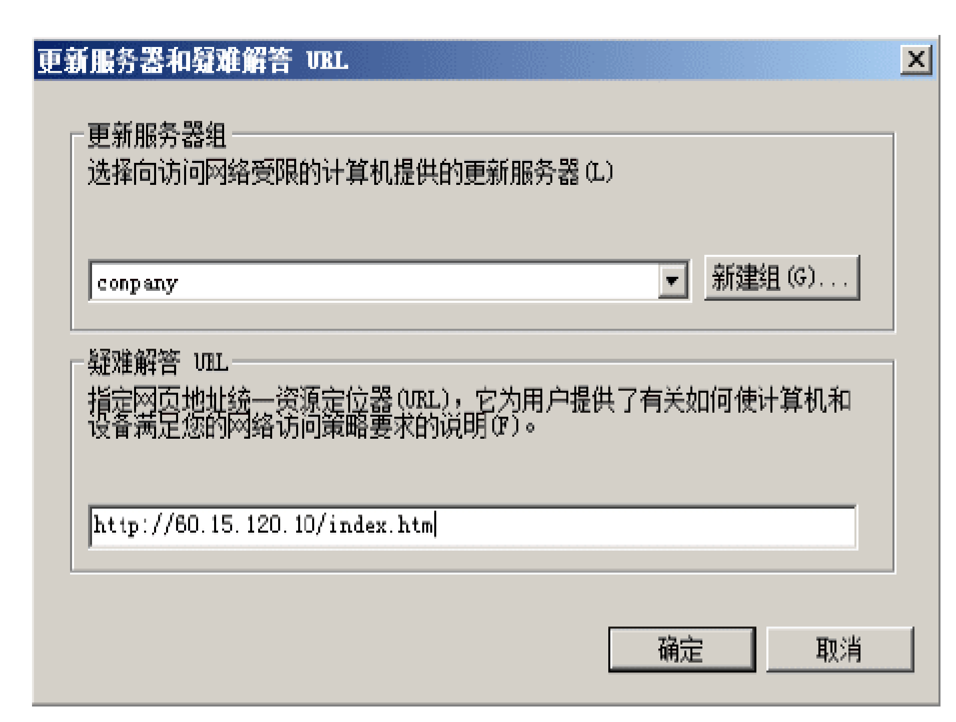


图 16.54 “更新服务器和疑难解答 URL”对话框

16.5.3 配置 DHCP 强制客户端

DHCP 强制客户端的配置过程与 IPSec 强制客户端类似，不同的是，在配置 NAP 客户端代理组件时，应启用“DHCP 隔离强制客户端”选项，如图 16.55 所示。其他配置操作完全相同，此处不复赘述。

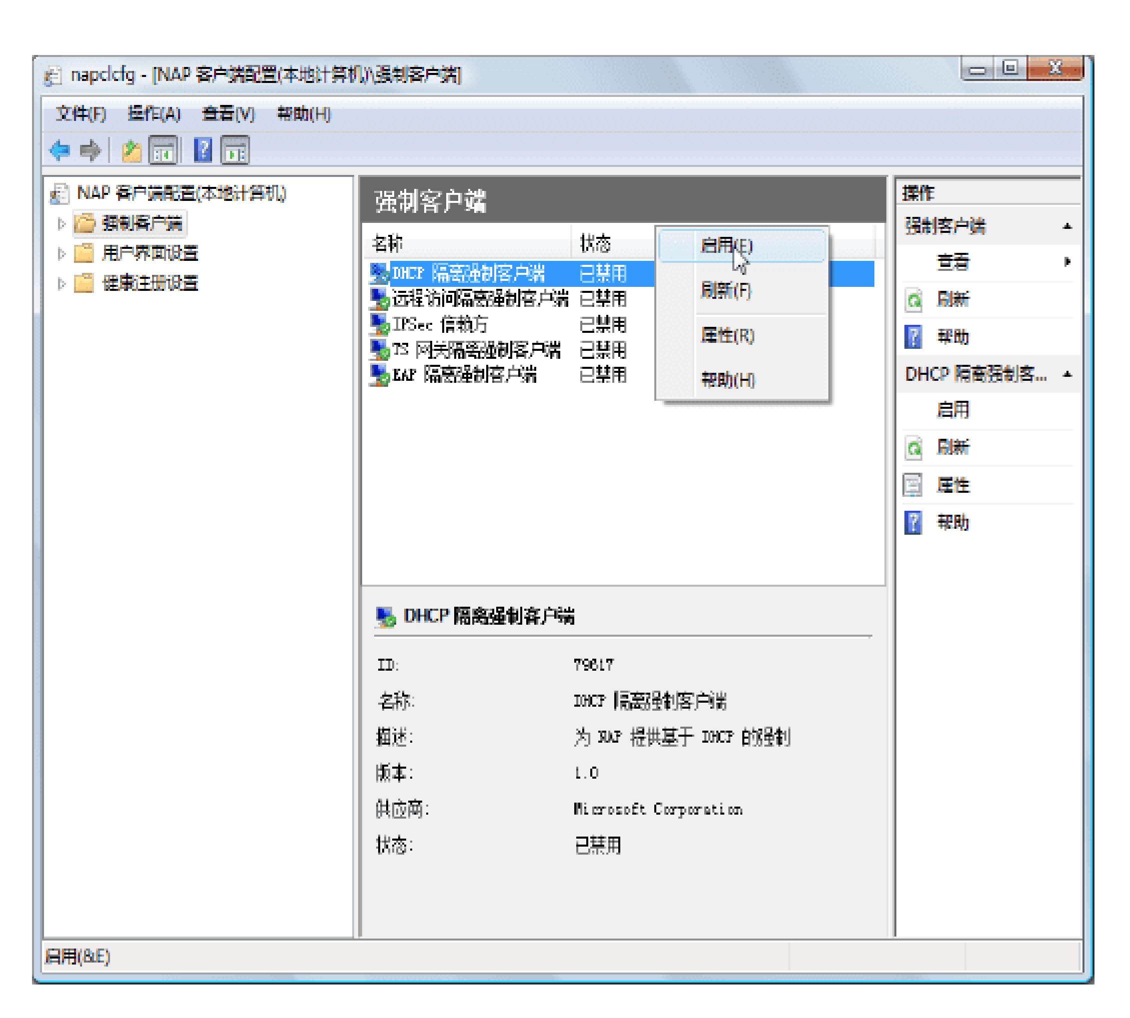


图 16.55 启用“DHCP 隔离强制客户端”

16.5.4 测试 DHCP 强制

如果客户端在没有开启系统防火墙或者没有开启自动更新的情况下，登录域控制器后，任务栏中会提示“此计算机不符合该网络策略的要求”。说明 NAP 服务器开始发挥作用了。此时该客户端不能继续访问网络中的某些服务器或计算机。单击提示信息，打开如图 16.56 所示“网络访问保护”对话框。该窗口中提示当前客户端未能通过网络策略检测的原因，并给出解



图 16.53 “配置设置”对话框

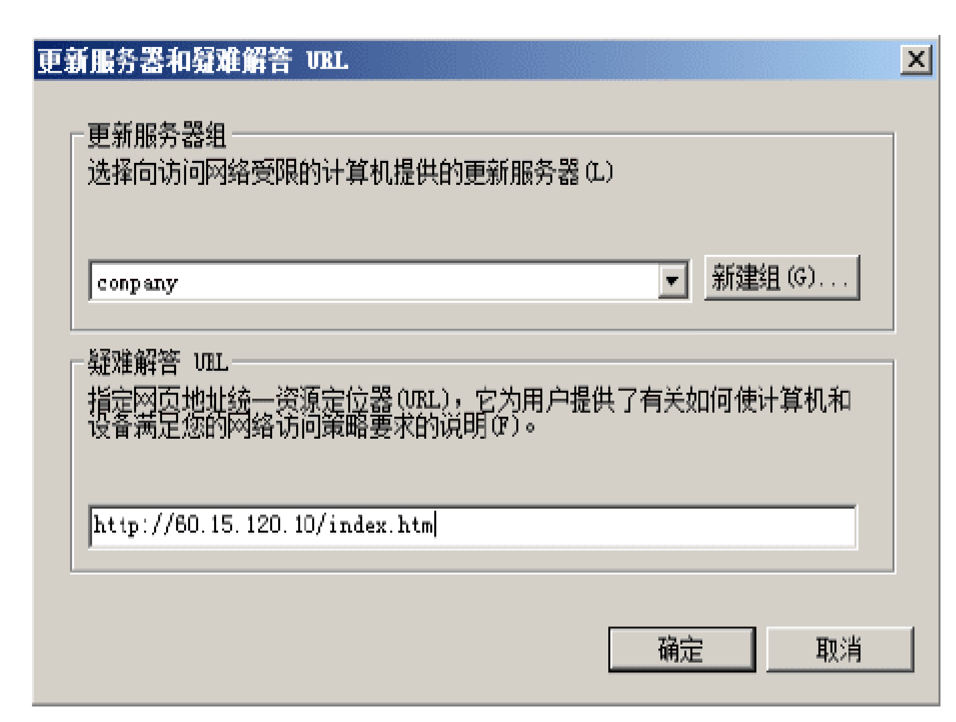


图 16.54 “更新服务器和疑难解答 URL”对话框

16.5.3 配置 DHCP 强制客户端

DHCP 强制客户端的配置过程与 IPSec 强制客户端类似，不同的是，在配置 NAP 客户端代理组件时，应启用“DHCP 隔离强制客户端”选项，如图 16.55 所示。其他配置操作完全相同，此处不复赘述。

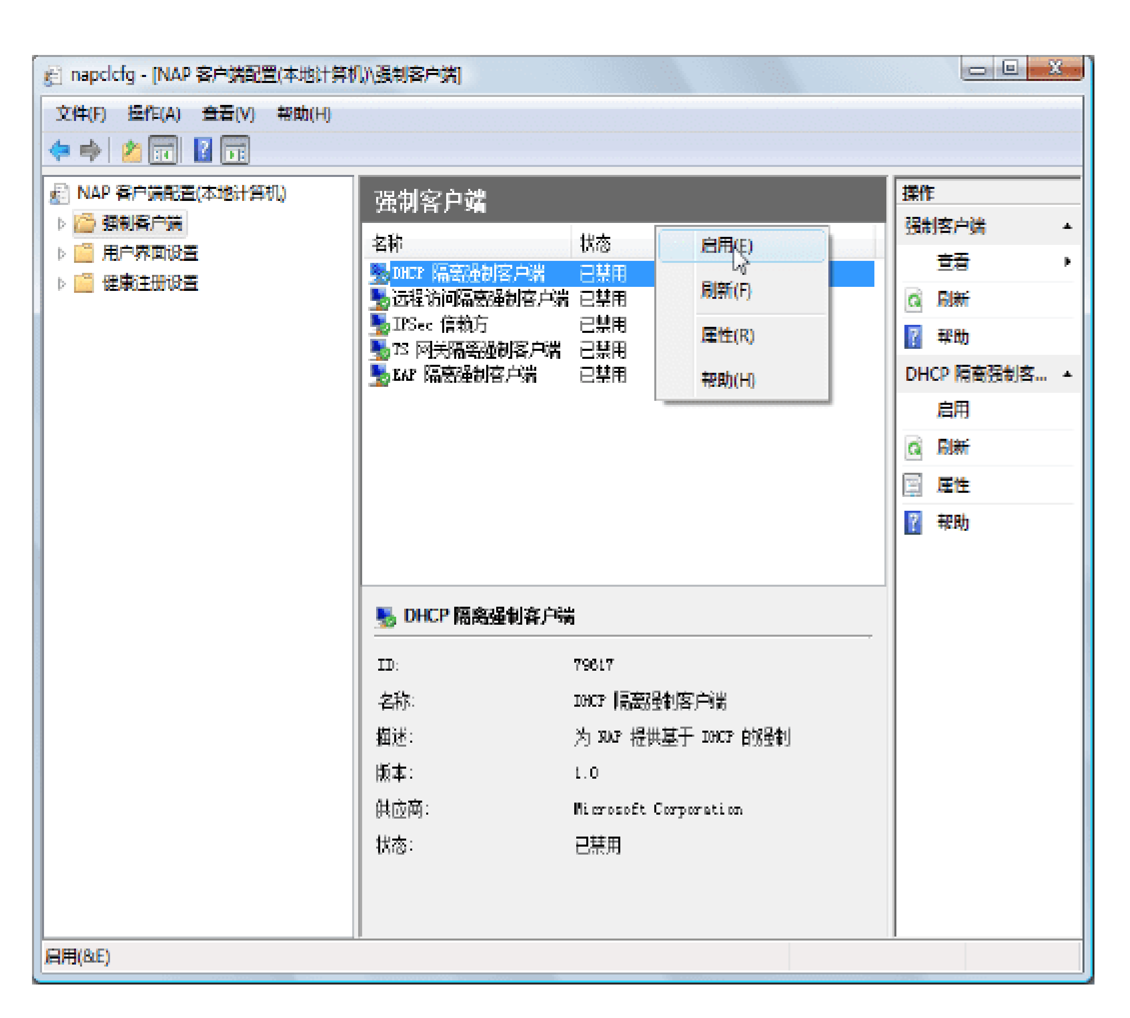


图 16.55 启用“DHCP 隔离强制客户端”

16.5.4 测试 DHCP 强制

如果客户端在没有开启系统防火墙或者没有开启自动更新的情况下，登录域控制器后，任务栏中会提示“此计算机不符合该网络策略的要求”。说明 NAP 服务器开始发挥作用了。此时该客户端不能继续访问网络中的某些服务器或计算机。单击提示信息，打开如图 16.56 所示“网络访问保护”对话框。该窗口中提示当前客户端未能通过网络策略检测的原因，并给出解



图 16.53 “配置设置”对话框

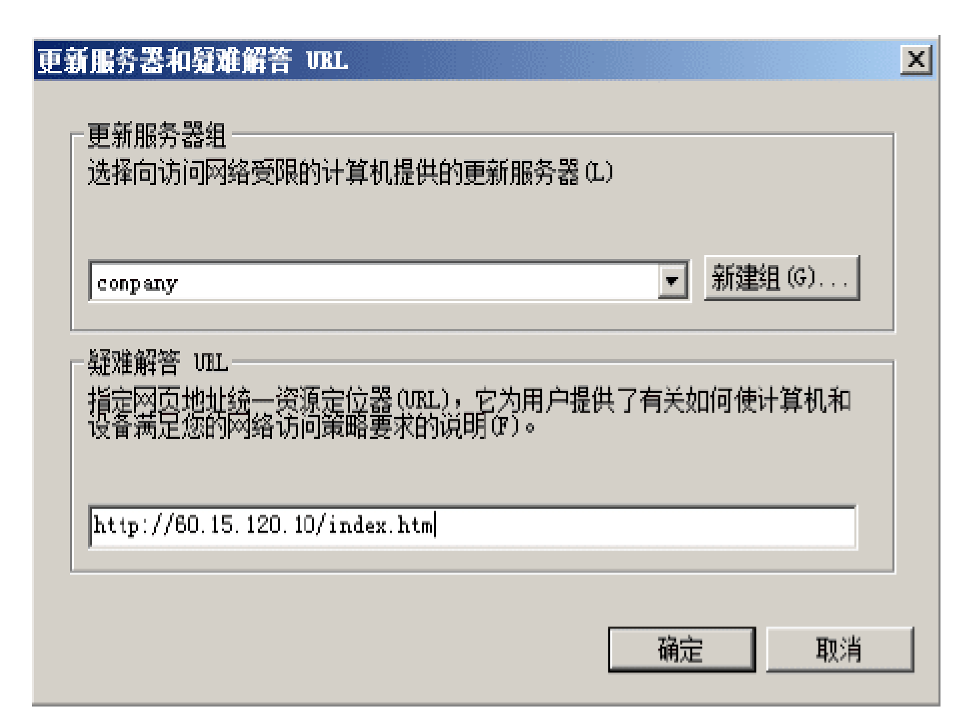


图 16.54 “更新服务器和疑难解答 URL”对话框

16.5.3 配置 DHCP 强制客户端

DHCP 强制客户端的配置过程与 IPSec 强制客户端类似，不同的是，在配置 NAP 客户端代理组件时，应启用“DHCP 隔离强制客户端”选项，如图 16.55 所示。其他配置操作完全相同，此处不复赘述。

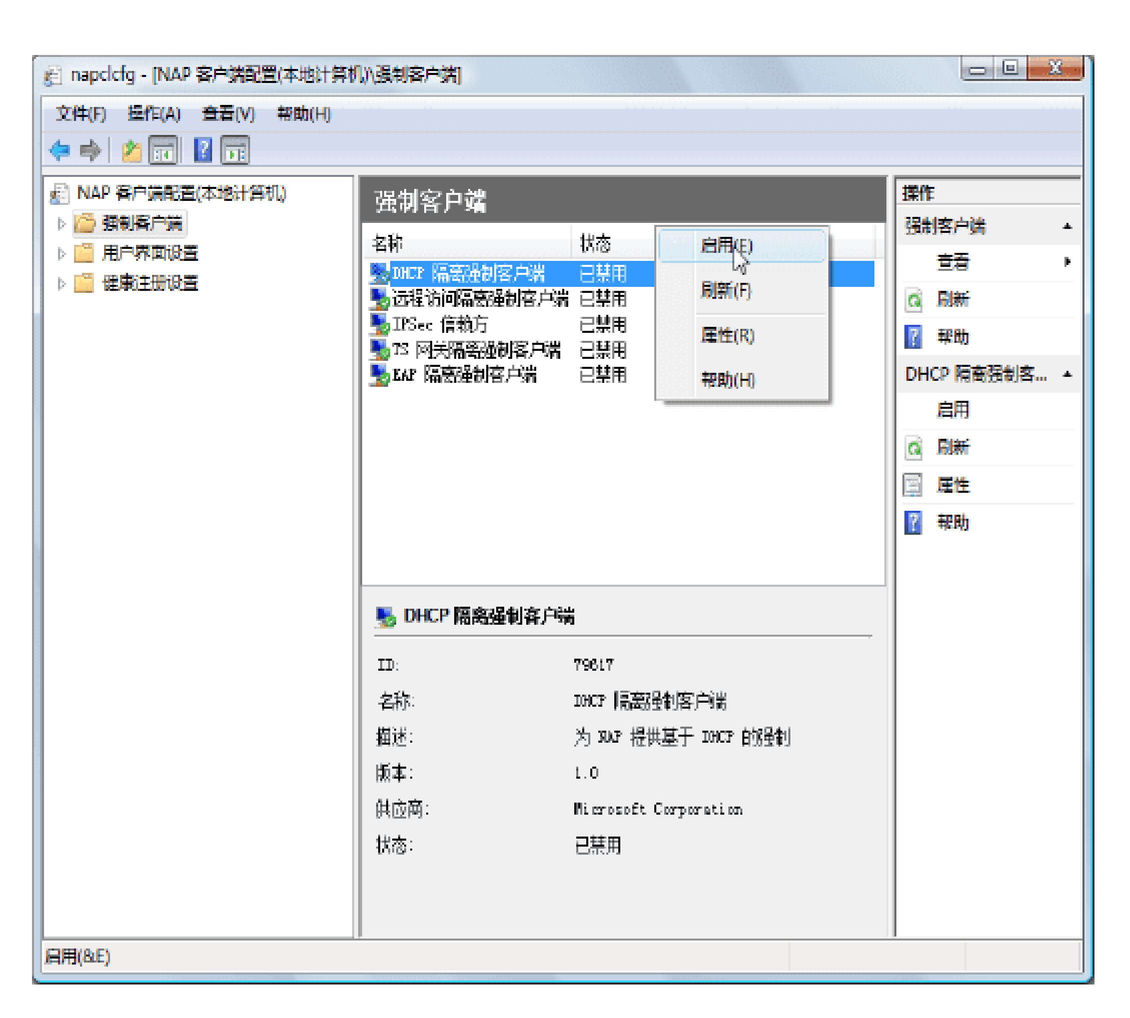


图 16.55 启用“DHCP 隔离强制客户端”

16.5.4 测试 DHCP 强制

如果客户端在没有开启系统防火墙或者没有开启自动更新的情况下，登录域控制器后，任务栏中会提示“此计算机不符合该网络策略的要求”。说明 NAP 服务器开始发挥作用了。此时该客户端不能继续访问网络中的某些服务器或计算机。单击提示信息，打开如图 16.56 所示“网络访问保护”对话框。该窗口中提示当前客户端未能通过网络策略检测的原因，并给出解



决问题的方案。这些提示方法就是系统健康策略模板中管理员设定的处理操作。



图 16.56　不符合策略要求的客户端提示信息

用户可以根据提示信息尝试解决相关问题，如开启系统防火墙、恶意软件保护功能或将系统升级到最新等。处理完毕后，任务栏中会提示“此计算机符合该网络的要求”。单击提示信息，会显示如图 16.57 所示“网络访问保护”对话框，已具有完全的网络访问权限。

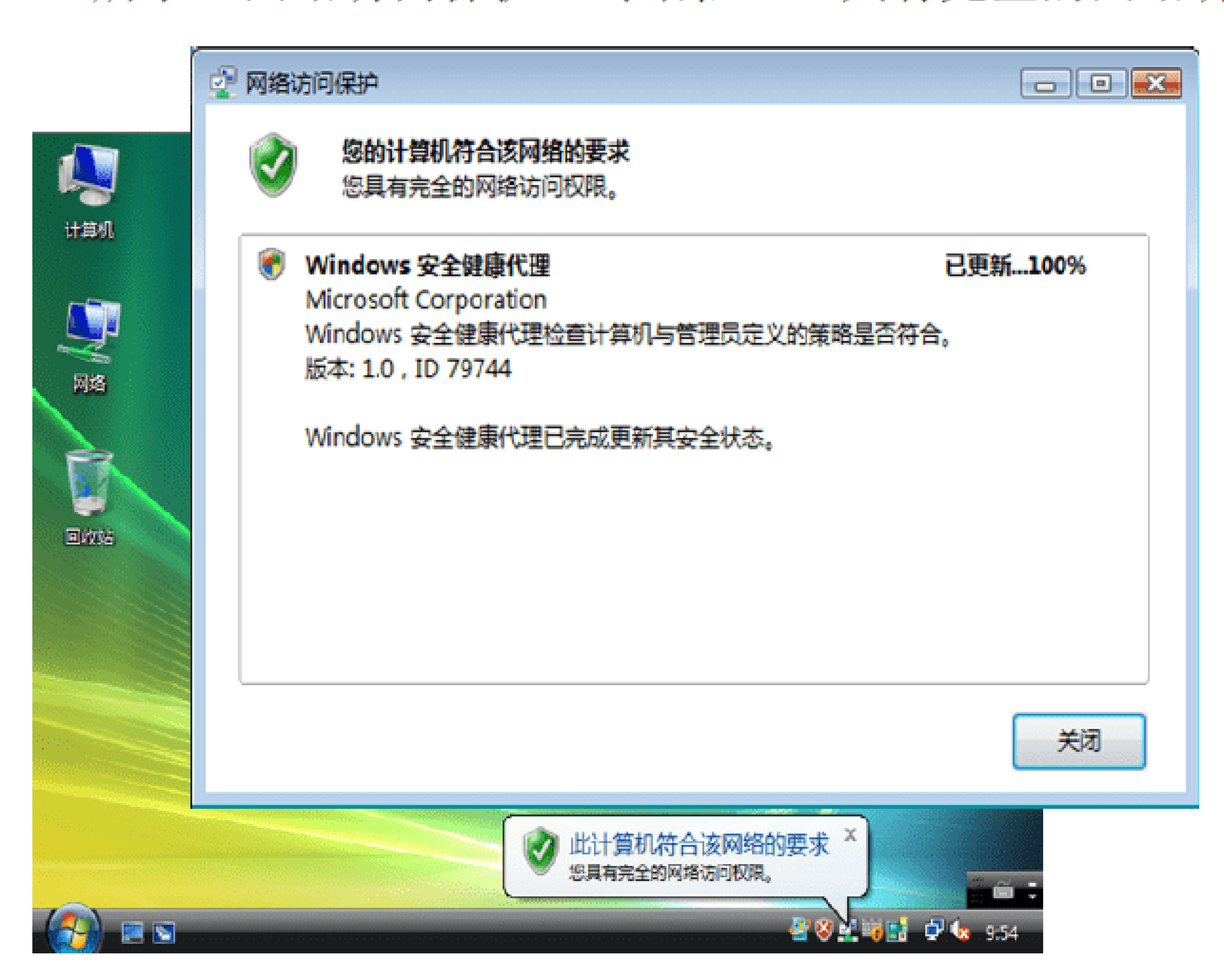


图 16.57　符合网络策略要求时的提示信息

16.6　配置 VPN 强制

VPN（Virtual Private Network，虚拟专用网）是目前常用的远程访问技术之一，主要特点就是传输安全性高，机制灵活。管理员可以借助 Windows Server 2008 提供的“路由和远程访问”服务，搭建和配置远程访问服务器，该角色默认并未安装。用户可以根据自己的需要选择同时安装网络策略和访问服务中的所有服务组件，或者只安装路由和远程访问服务。

16.6.1 远程访问 VPN 服务器的配置

VPN 服务器是 VPN 强制系统中的重要角色。默认情况下，VPN 服务器可以对远程用户的拨入请求进行简单的身份验证，如验证用户名、密码等。如果与 NPS 服务器配合使用，需要对其身份验证方式进行修改，使其将身份验证请求发送到 NPS 服务器，从而实现联合工作。

1. 安装和配置远程访问 VPN 服务器

VPN 服务器用来提供拨入功能，供远程计算机用户拨入公司局域网。不过，VPN 服务可以与网络策略服务器配合使用，对拨入的客户端用户进行验证，只允许通过网络安全验证的计算机才允许访问网络。VPN 服务器上需要安装两块网卡，一块网卡设置内网地址，用来连接局域网；另一块设置公网地址，用来连接 Internet。

01 运行“添加角色向导”链接，在“选择服务器角色”对话框中，选择“网络策略和访问服务”角色。依次单击“下一步”按钮，在“选择角色服务”对话框中，选中“网络策略服务器”和“路由和远程访问服务”复选框，其他选项保持默认即可，直至安装完成。如图 16.58 所示。

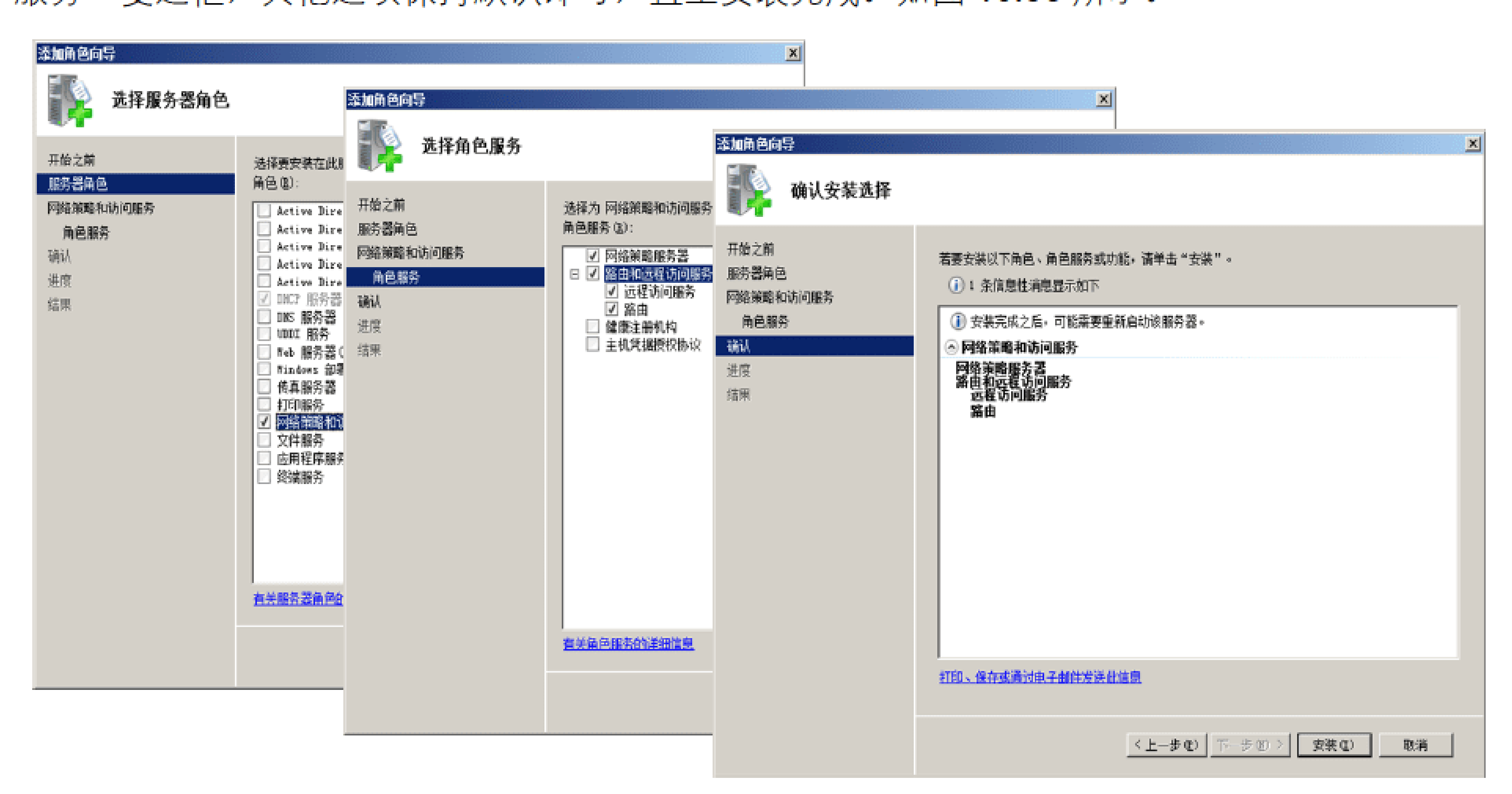


图 16.58 安装路由和远程访问服务

02 安装完成的“路由和远程访问服务”是禁用的，需要管理员手动启用并配置。依次单击“开始”→“管理工具”→“路由和远程访问”，打开“路由和远程访问”控制台窗口，默认是未配置的，右击服务器名并选择“配置并启用路由和远程访问”，即可启动路由和远程访问服务器安装向导。依次单击“下一步”按钮，设置远程访问方法和类型，如图 16.59 所示。



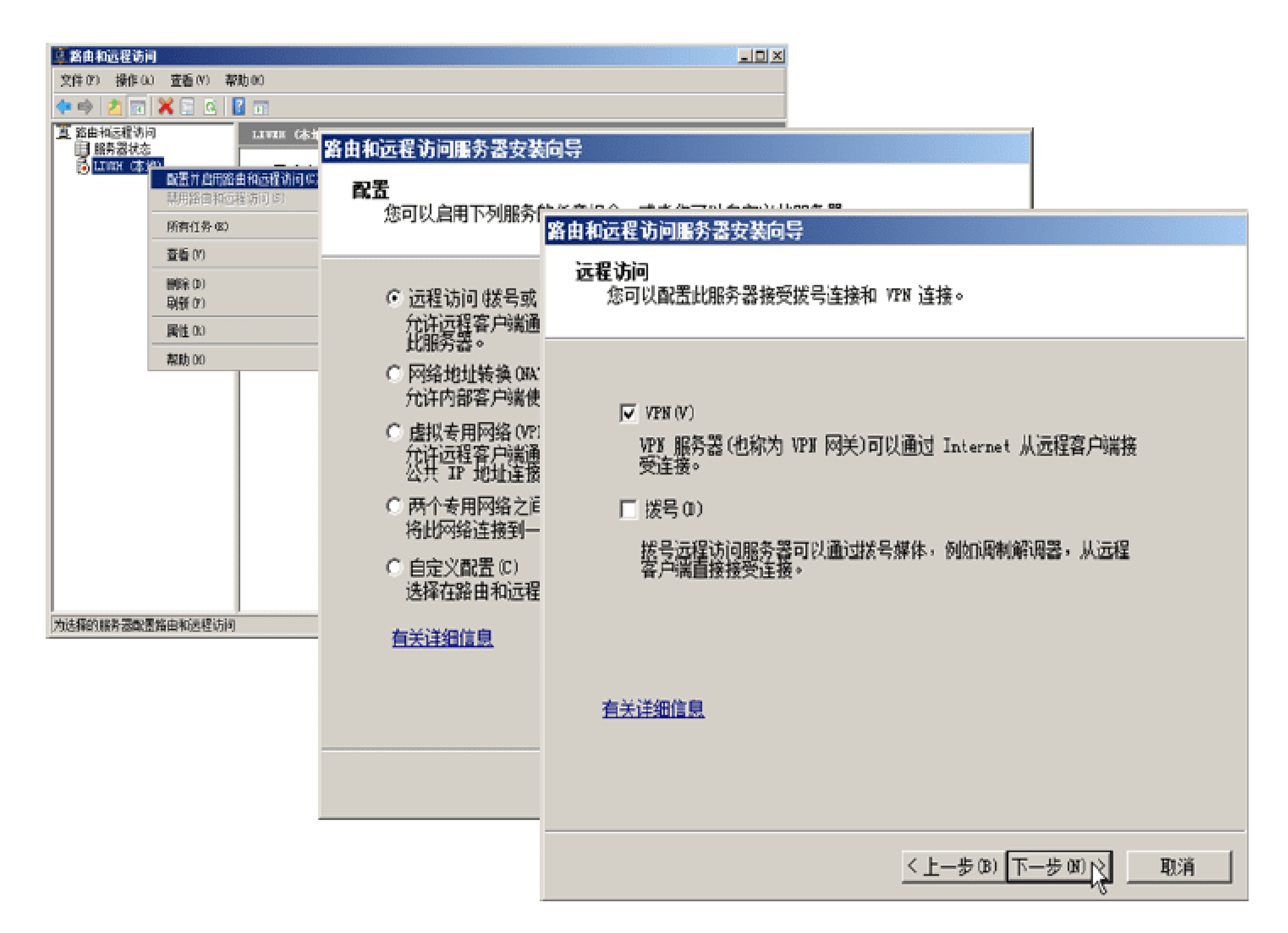


图 16.59　配置远程访问方法和类型

03 依次单击“下一步”按钮，设置 VPN 远程访问服务器的网络连接和 IP 地址分配方式，如图 16.60 所示。配置 VPN 远程访问服务器至少提供两块网卡，即一块连接 Internet，相应远程用户的访问，另一块用于连接内网。在“网络接口”列表中选择此服务连接到 Internet 的连接即可。管理员可以指定远程客户端获得 IP 地址的方式，如果本地网络中已经配置 DHCP 服务器，可以选择“自动”方式，客户端可以从 DHCP 服务器获得内网 IP 地址。否则，可以选择“来自一个指定的地址范围”单选按钮。

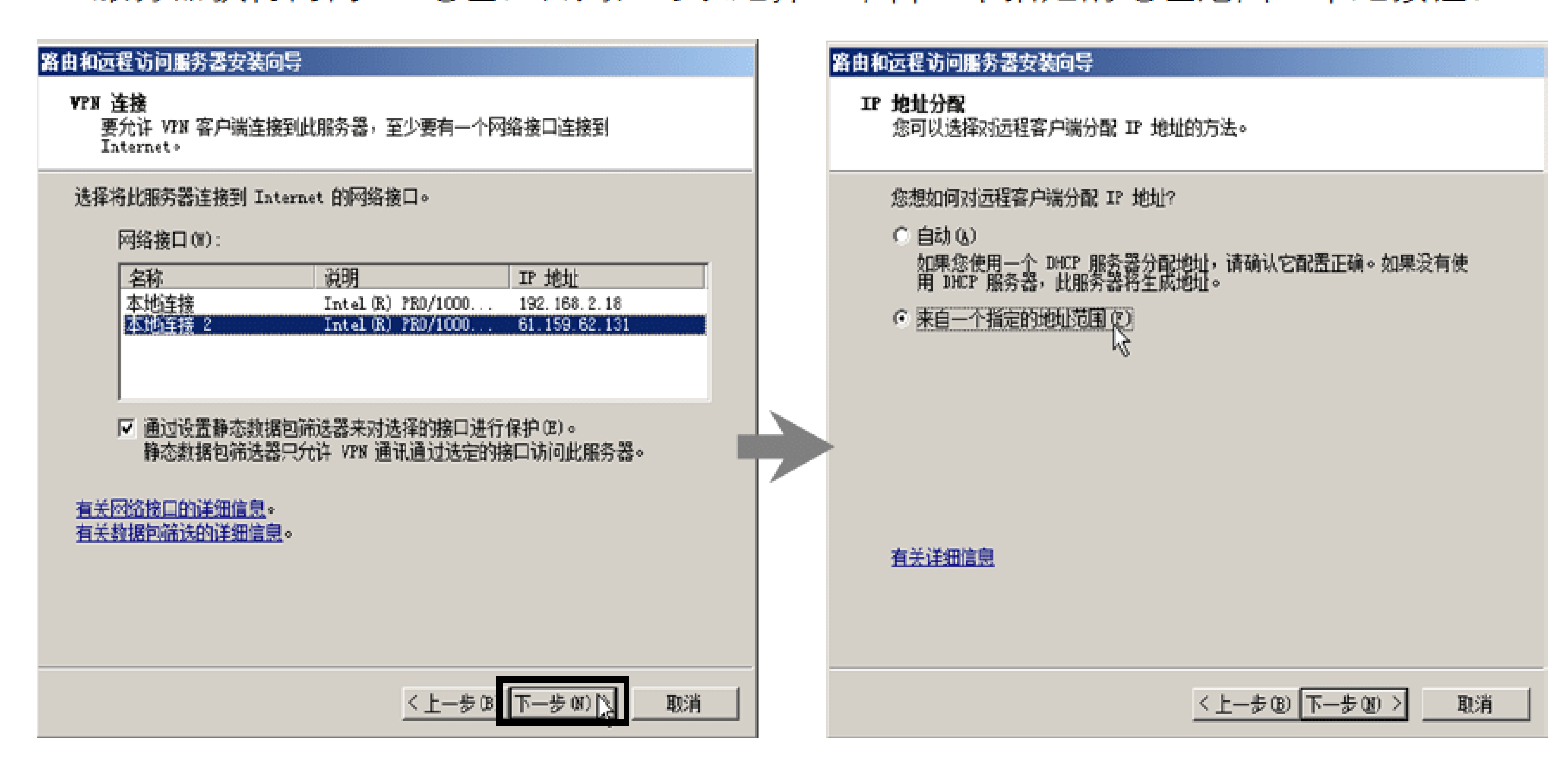


图 16.60　VPN 连接 IP 地址分配

04 单击“下一步”按钮，显示“管理多个远程访问服务器”对话框。如果计划在专用网络上安装多个 VPN 服务器、无线访问点或其他 RADIUS 客户端，添加 RADIUS 服务器非常有用。否则保留默认的“否，使用路由和远程访问来对连接请求进行身份验证”单选按钮即可。该选择将服务器配置为使用 Windows 身份验证、Windows 记账和本地存储的远程访问策略，在本地对连接请求进行身份验证。继续单击“下一步”按钮，即可完成 VPN 服务器配置，此时会提示用户在设置远程访问服务器以后，需要再指定 DHCP 服务器的 IP 地址。如图 16.61 所示。



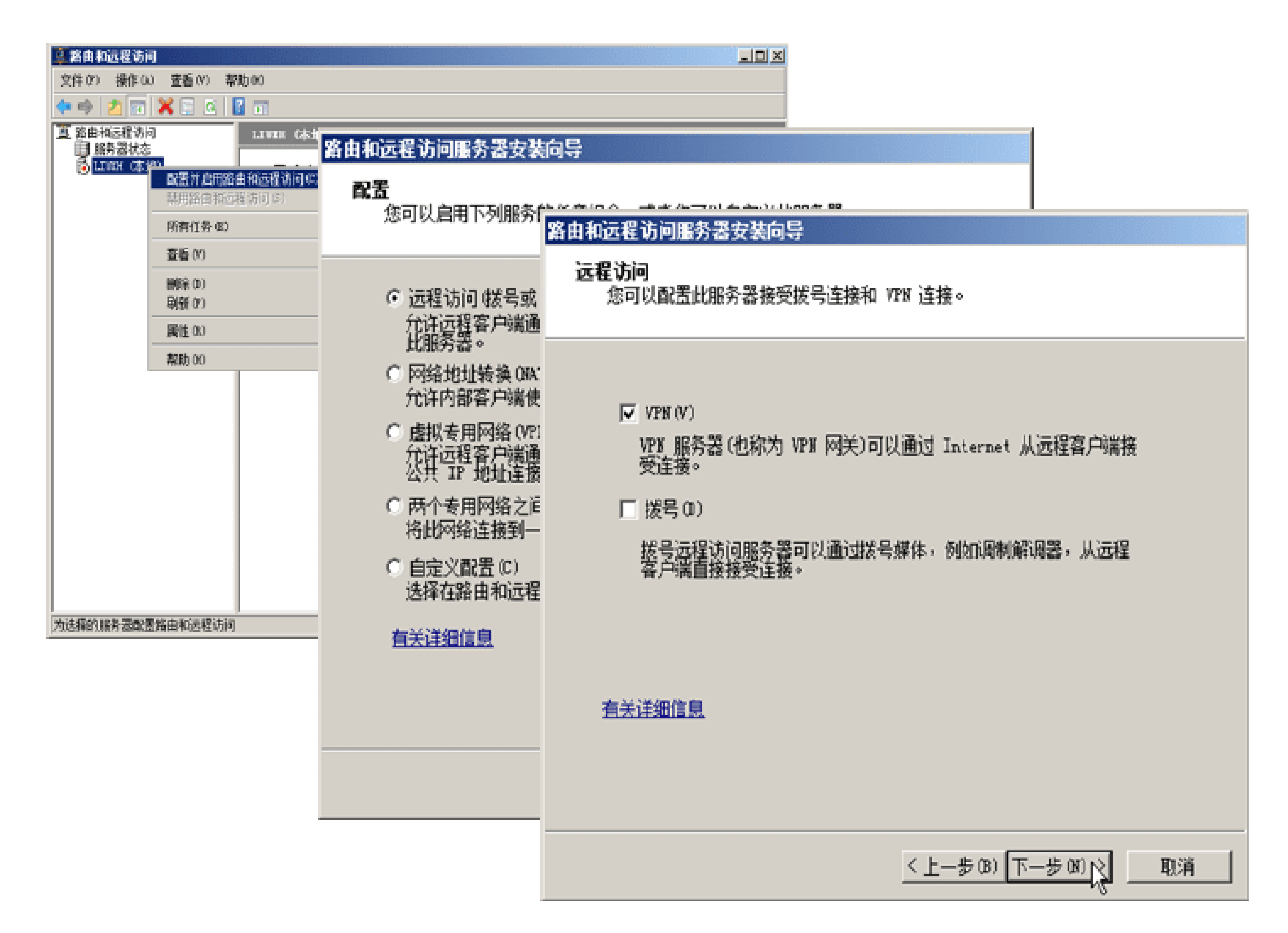


图 16.59　配置远程访问方法和类型

03 依次单击“下一步”按钮，设置 VPN 远程访问服务器的网络连接和 IP 地址分配方式，如图 16.60 所示。配置 VPN 远程访问服务器至少提供两块网卡，即一块连接 Internet，相应远程用户的访问，另一块用于连接内网。在“网络接口”列表中选择此服务连接到 Internet 的连接即可。管理员可以指定远程客户端获得 IP 地址的方式，如果本地网络中已经配置 DHCP 服务器，可以选择“自动”方式，客户端可以从 DHCP 服务器获得内网 IP 地址。否则，可以选择“来自一个指定的地址范围”单选按钮。

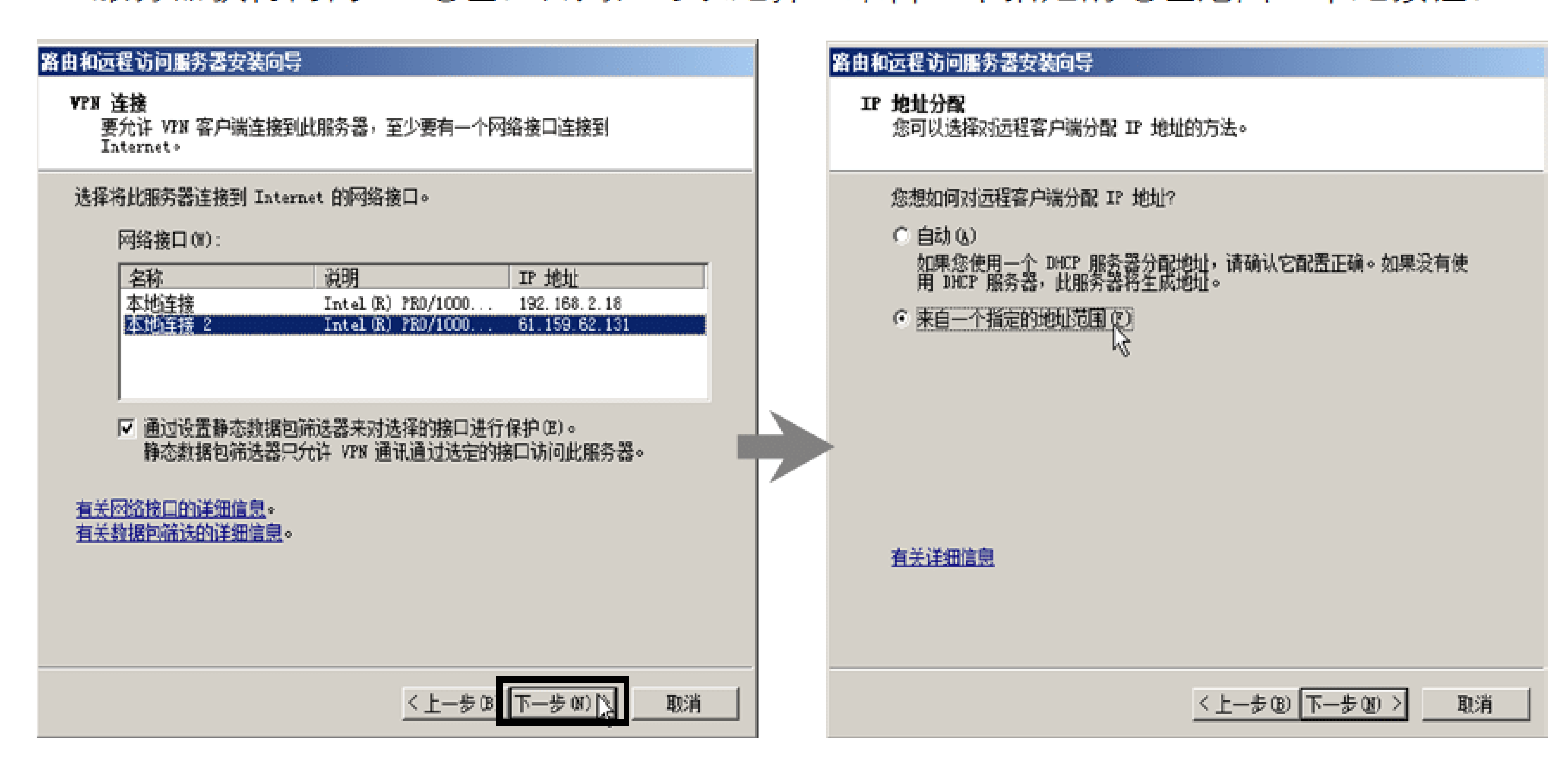


图 16.60　VPN 连接 IP 地址分配

04 单击“下一步”按钮，显示“管理多个远程访问服务器”对话框。如果计划在专用网络上安装多个 VPN 服务器、无线访问点或其他 RADIUS 客户端，添加 RADIUS 服务器非常有用。否则保留默认的“否，使用路由和远程访问来对连接请求进行身份验证”单选按钮即可。该选择将服务器配置为使用 Windows 身份验证、Windows 记账和本地存储的远程访问策略，在本地对连接请求进行身份验证。继续单击“下一步”按钮，即可完成 VPN 服务器配置，此时会提示用户在设置远程访问服务器以后，需要再指定 DHCP 服务器的 IP 地址。如图 16.61 所示。



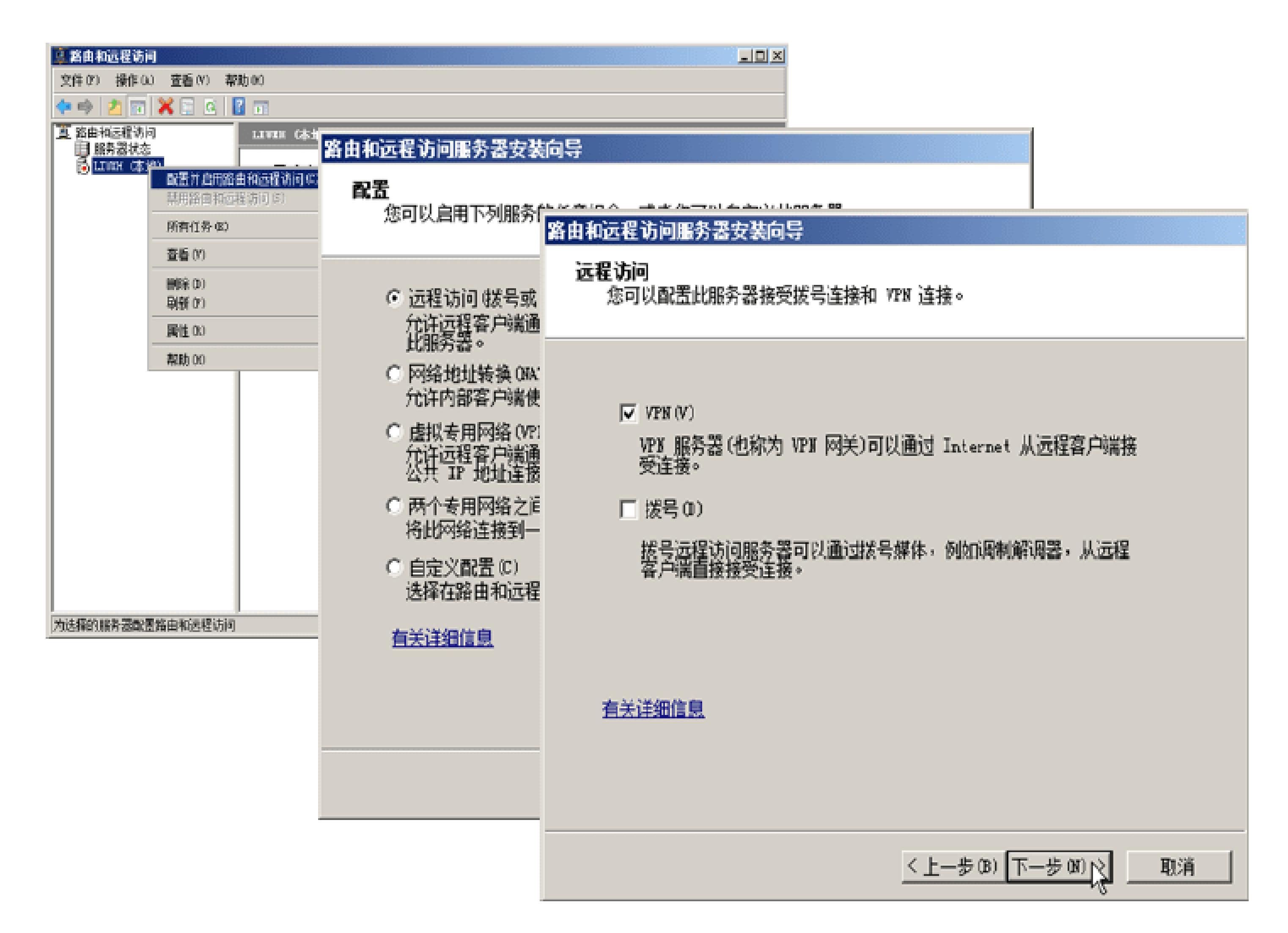


图 16.59　配置远程访问方法和类型

03 依次单击“下一步”按钮，设置 VPN 远程访问服务器的网络连接和 IP 地址分配方式，如图 16.60 所示。配置 VPN 远程访问服务器至少提供两块网卡，即一块连接 Internet，相应远程用户的访问，另一块用于连接内网。在“网络接口”列表中选择此服务连接到 Internet 的连接即可。管理员可以指定远程客户端获得 IP 地址的方式，如果本地网络中已经配置 DHCP 服务器，可以选择“自动”方式，客户端可以从 DHCP 服务器获得内网 IP 地址。否则，可以选择“来自一个指定的地址范围”单选按钮。

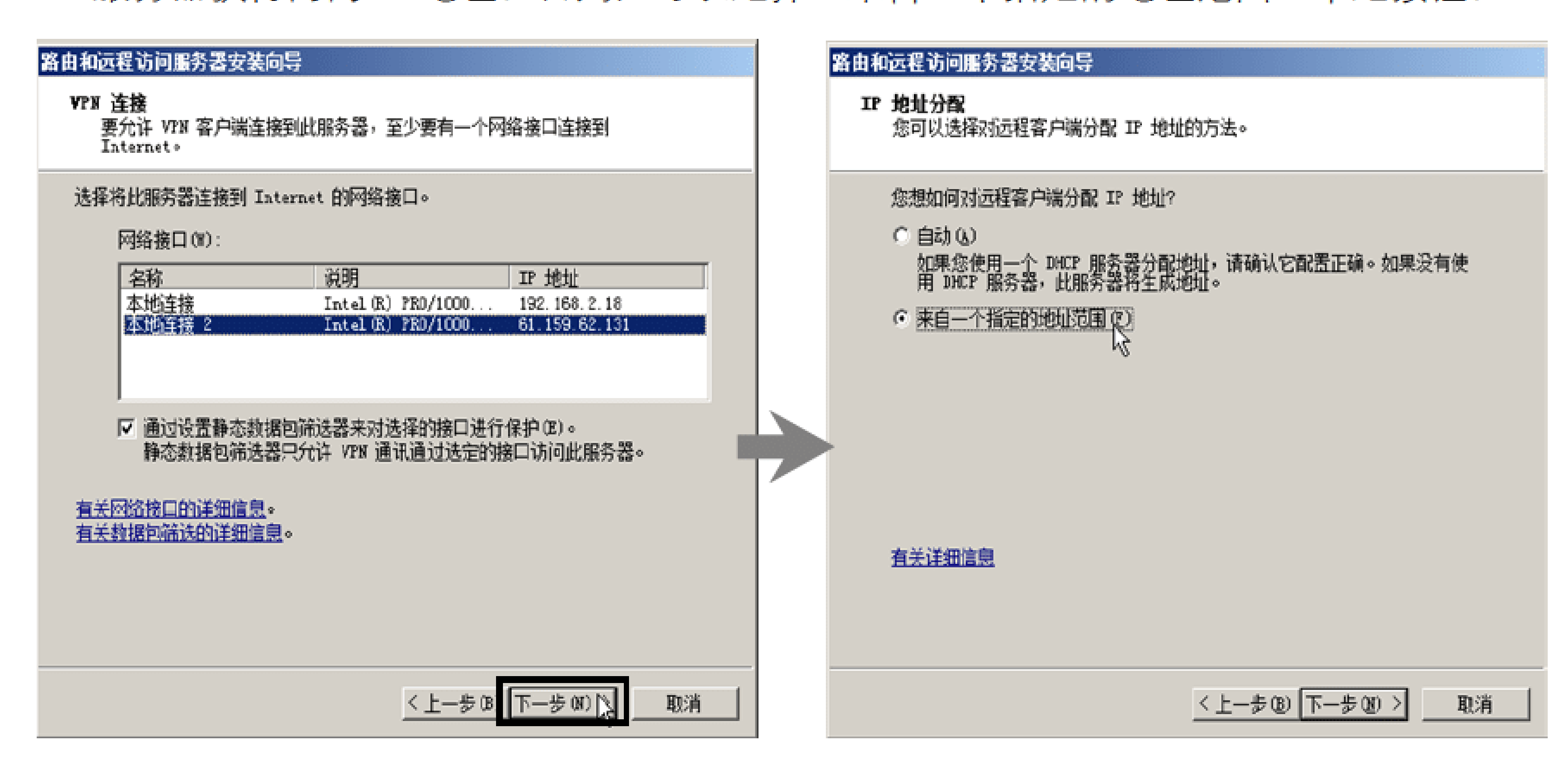


图 16.60　VPN 连接 IP 地址分配

04 单击“下一步”按钮，显示“管理多个远程访问服务器”对话框。如果计划在专用网络上安装多个 VPN 服务器、无线访问点或其他 RADIUS 客户端，添加 RADIUS 服务器非常有用。否则保留默认的“否，使用路由和远程访问来对连接请求进行身份验证”单选按钮即可。该选择将服务器配置为使用 Windows 身份验证、Windows 记账和本地存储的远程访问策略，在本地对连接请求进行身份验证。继续单击“下一步”按钮，即可完成 VPN 服务器配置，此时会提示用户在设置远程访问服务器以后，需要再指定 DHCP 服务器的 IP 地址。如图 16.61 所示。



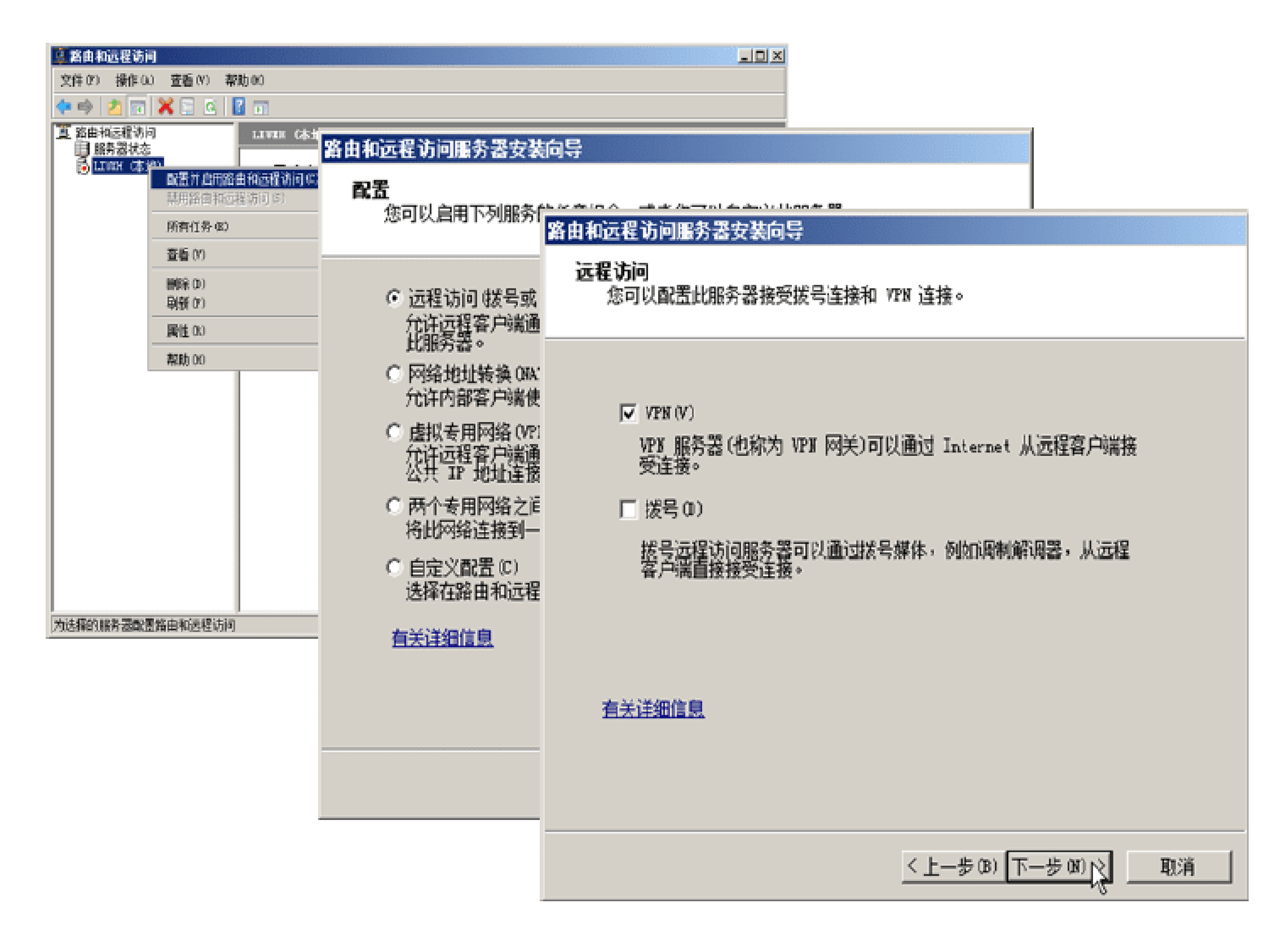


图 16.59　配置远程访问方法和类型

03 依次单击“下一步”按钮，设置 VPN 远程访问服务器的网络连接和 IP 地址分配方式，如图 16.60 所示。配置 VPN 远程访问服务器至少提供两块网卡，即一块连接 Internet，相应远程用户的访问，另一块用于连接内网。在“网络接口”列表中选择此服务连接到 Internet 的连接即可。管理员可以指定远程客户端获得 IP 地址的方式，如果本地网络中已经配置 DHCP 服务器，可以选择“自动”方式，客户端可以从 DHCP 服务器获得内网 IP 地址。否则，可以选择“来自一个指定的地址范围”单选按钮。

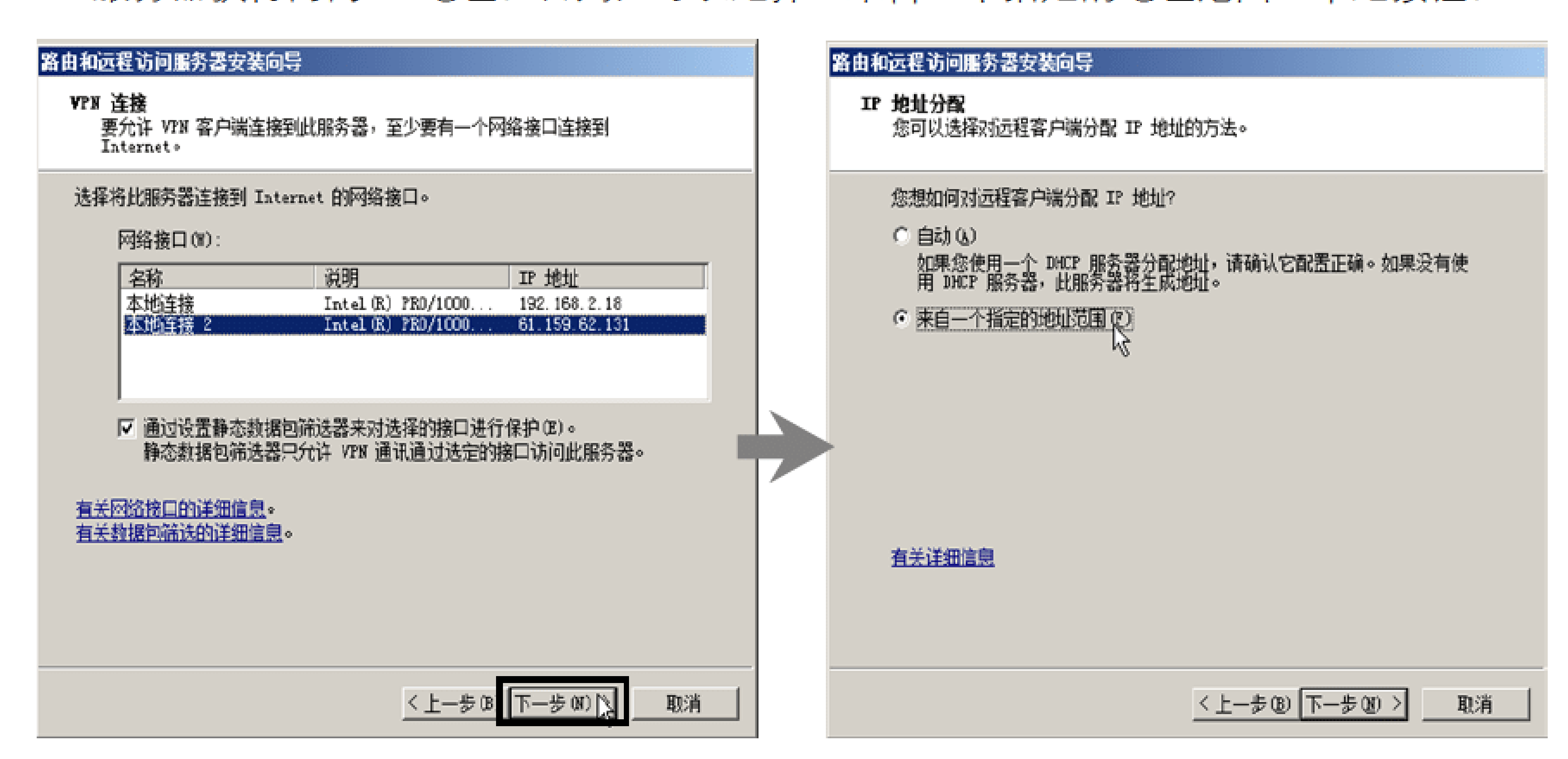


图 16.60　VPN 连接 IP 地址分配

04 单击“下一步”按钮，显示“管理多个远程访问服务器”对话框。如果计划在专用网络上安装多个 VPN 服务器、无线访问点或其他 RADIUS 客户端，添加 RADIUS 服务器非常有用。否则保留默认的“否，使用路由和远程访问来对连接请求进行身份验证”单选按钮即可。该选择将服务器配置为使用 Windows 身份验证、Windows 记账和本地存储的远程访问策略，在本地对连接请求进行身份验证。继续单击“下一步”按钮，即可完成 VPN 服务器配置，此时会提示用户在设置远程访问服务器以后，需要再指定 DHCP 服务器的 IP 地址。如图 16.61 所示。



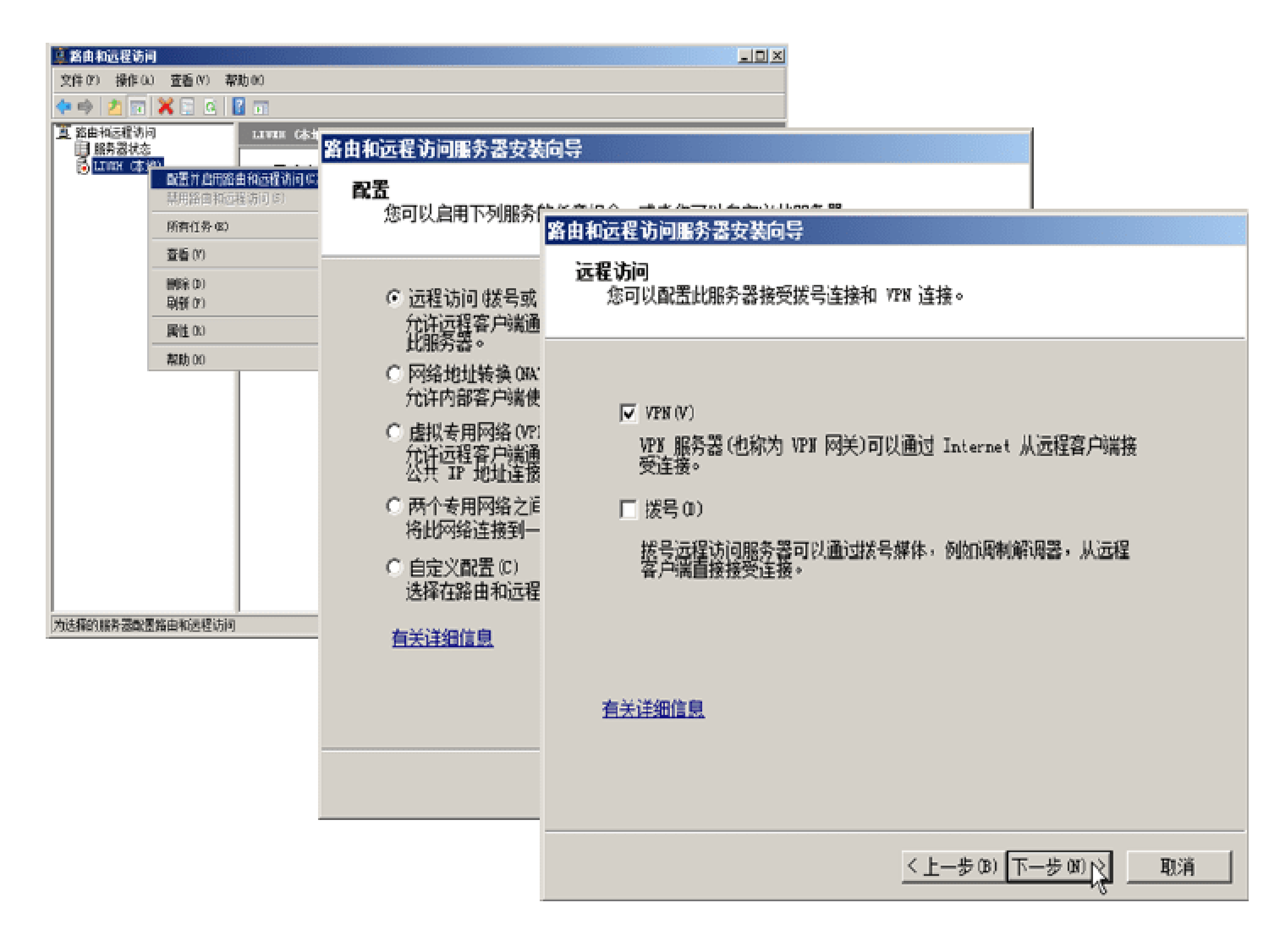


图 16.59　配置远程访问方法和类型

03 依次单击“下一步”按钮，设置 VPN 远程访问服务器的网络连接和 IP 地址分配方式，如图 16.60 所示。配置 VPN 远程访问服务器至少提供两块网卡，即一块连接 Internet，相应远程用户的访问，另一块用于连接内网。在“网络接口”列表中选择此服务连接到 Internet 的连接即可。管理员可以指定远程客户端获得 IP 地址的方式，如果本地网络中已经配置 DHCP 服务器，可以选择“自动”方式，客户端可以从 DHCP 服务器获得内网 IP 地址。否则，可以选择“来自一个指定的地址范围”单选按钮。

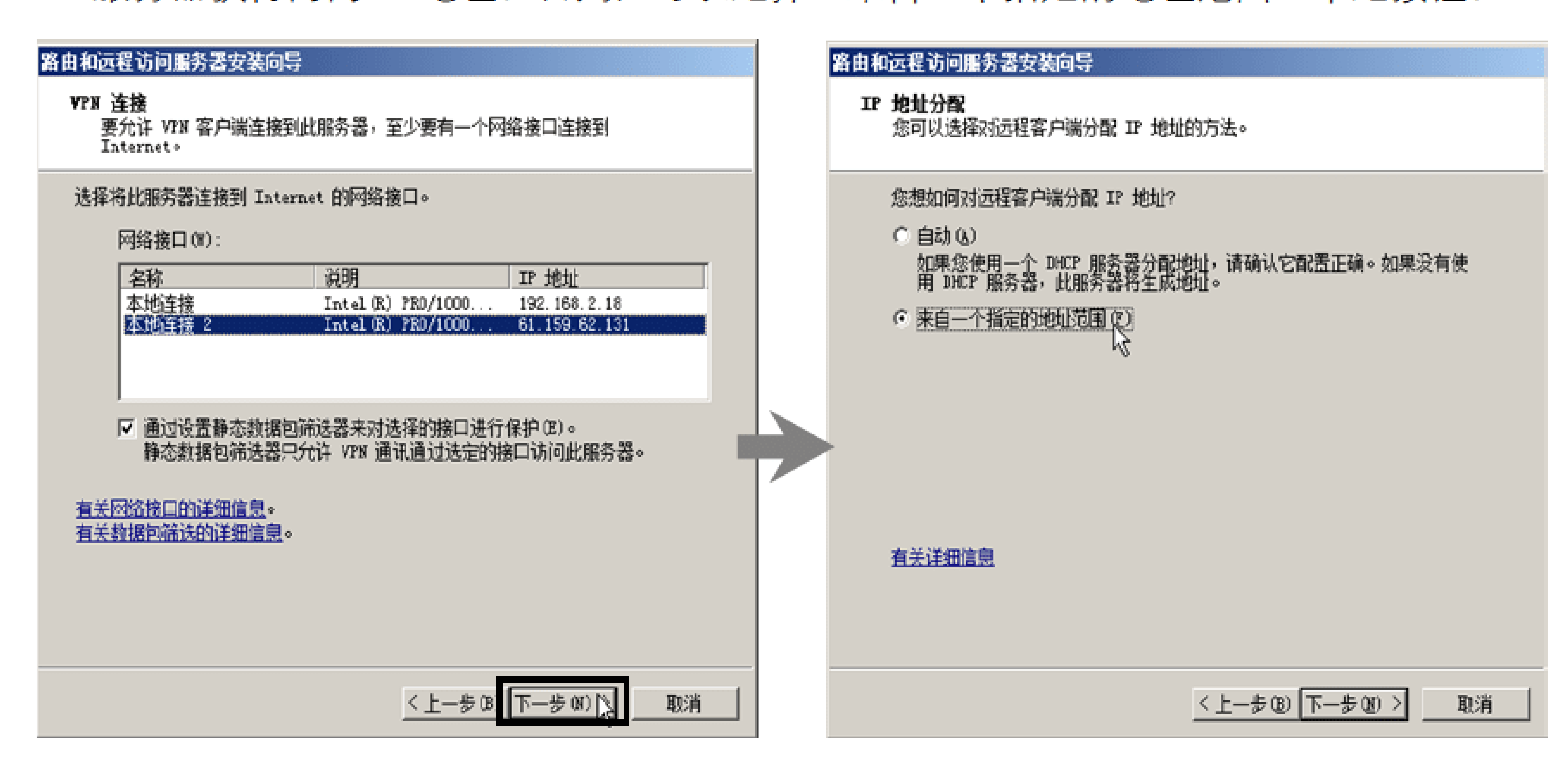


图 16.60　VPN 连接 IP 地址分配

04 单击“下一步”按钮，显示“管理多个远程访问服务器”对话框。如果计划在专用网络上安装多个 VPN 服务器、无线访问点或其他 RADIUS 客户端，添加 RADIUS 服务器非常有用。否则保留默认的“否，使用路由和远程访问来对连接请求进行身份验证”单选按钮即可。该选择将服务器配置为使用 Windows 身份验证、Windows 记账和本地存储的远程访问策略，在本地对连接请求进行身份验证。继续单击“下一步”按钮，即可完成 VPN 服务器配置，此时会提示用户在设置远程访问服务器以后，需要再指定 DHCP 服务器的 IP 地址。如图 16.61 所示。



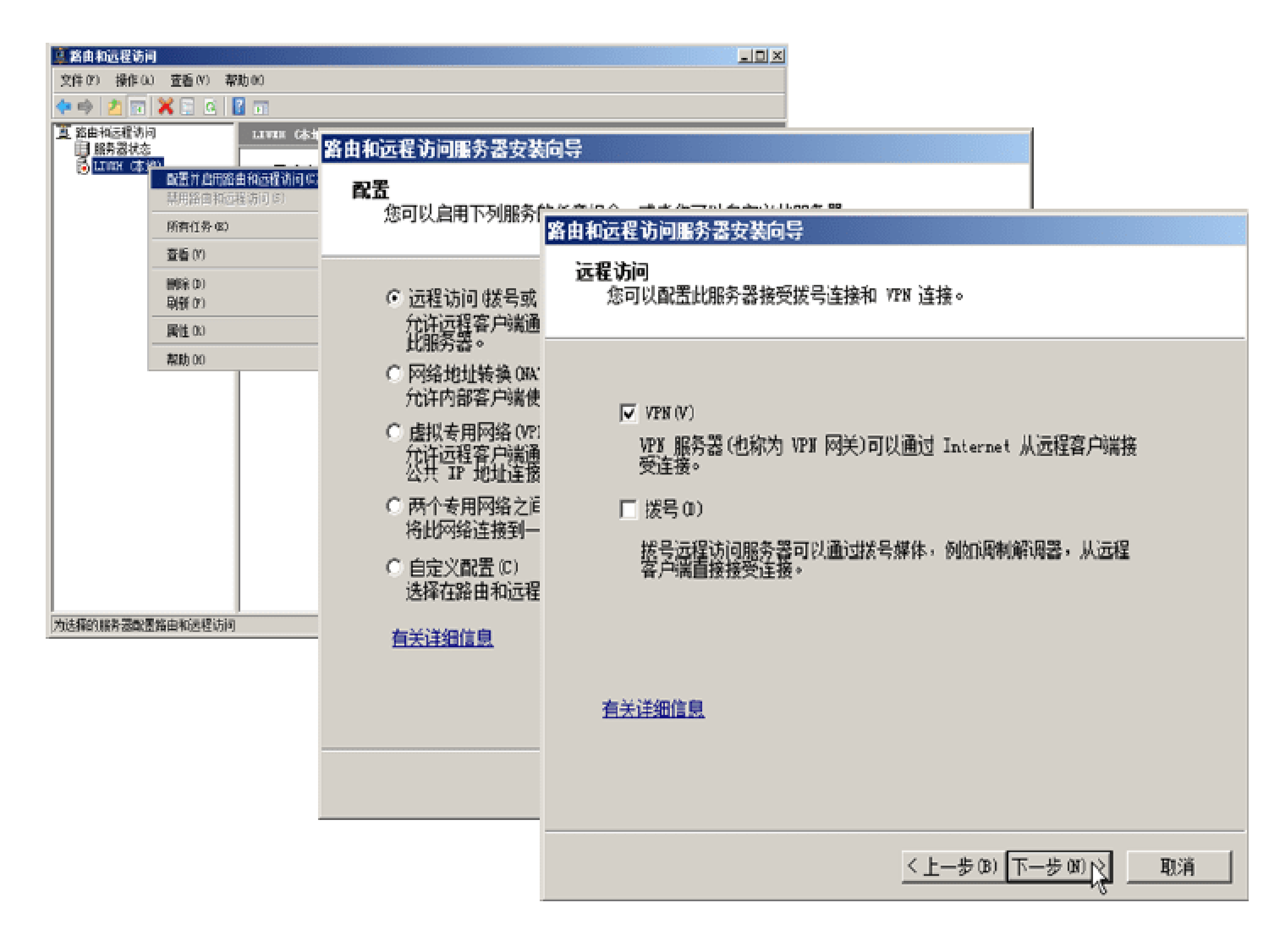


图 16.59　配置远程访问方法和类型

03 依次单击“下一步”按钮，设置 VPN 远程访问服务器的网络连接和 IP 地址分配方式，如图 16.60 所示。配置 VPN 远程访问服务器至少提供两块网卡，即一块连接 Internet，相应远程用户的访问，另一块用于连接内网。在“网络接口”列表中选择此服务连接到 Internet 的连接即可。管理员可以指定远程客户端获得 IP 地址的方式，如果本地网络中已经配置 DHCP 服务器，可以选择“自动”方式，客户端可以从 DHCP 服务器获得内网 IP 地址。否则，可以选择“来自一个指定的地址范围”单选按钮。

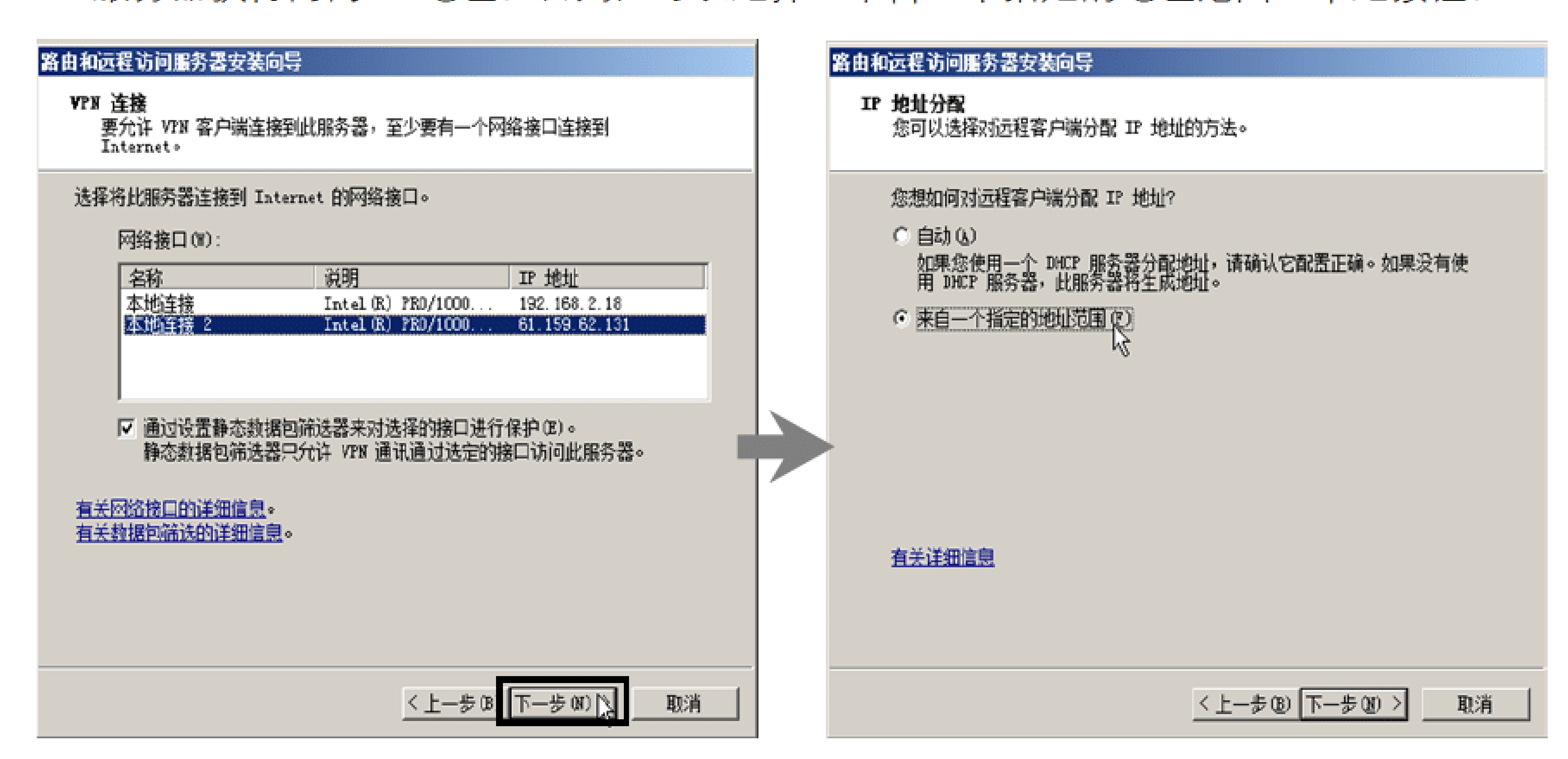


图 16.60　VPN 连接 IP 地址分配

04 单击“下一步”按钮，显示“管理多个远程访问服务器”对话框。如果计划在专用网络上安装多个 VPN 服务器、无线访问点或其他 RADIUS 客户端，添加 RADIUS 服务器非常有用。否则保留默认的“否，使用路由和远程访问来对连接请求进行身份验证”单选按钮即可。该选择将服务器配置为使用 Windows 身份验证、Windows 记账和本地存储的远程访问策略，在本地对连接请求进行身份验证。继续单击“下一步”按钮，即可完成 VPN 服务器配置，此时会提示用户在设置远程访问服务器以后，需要再指定 DHCP 服务器的 IP 地址。如图 16.61 所示。



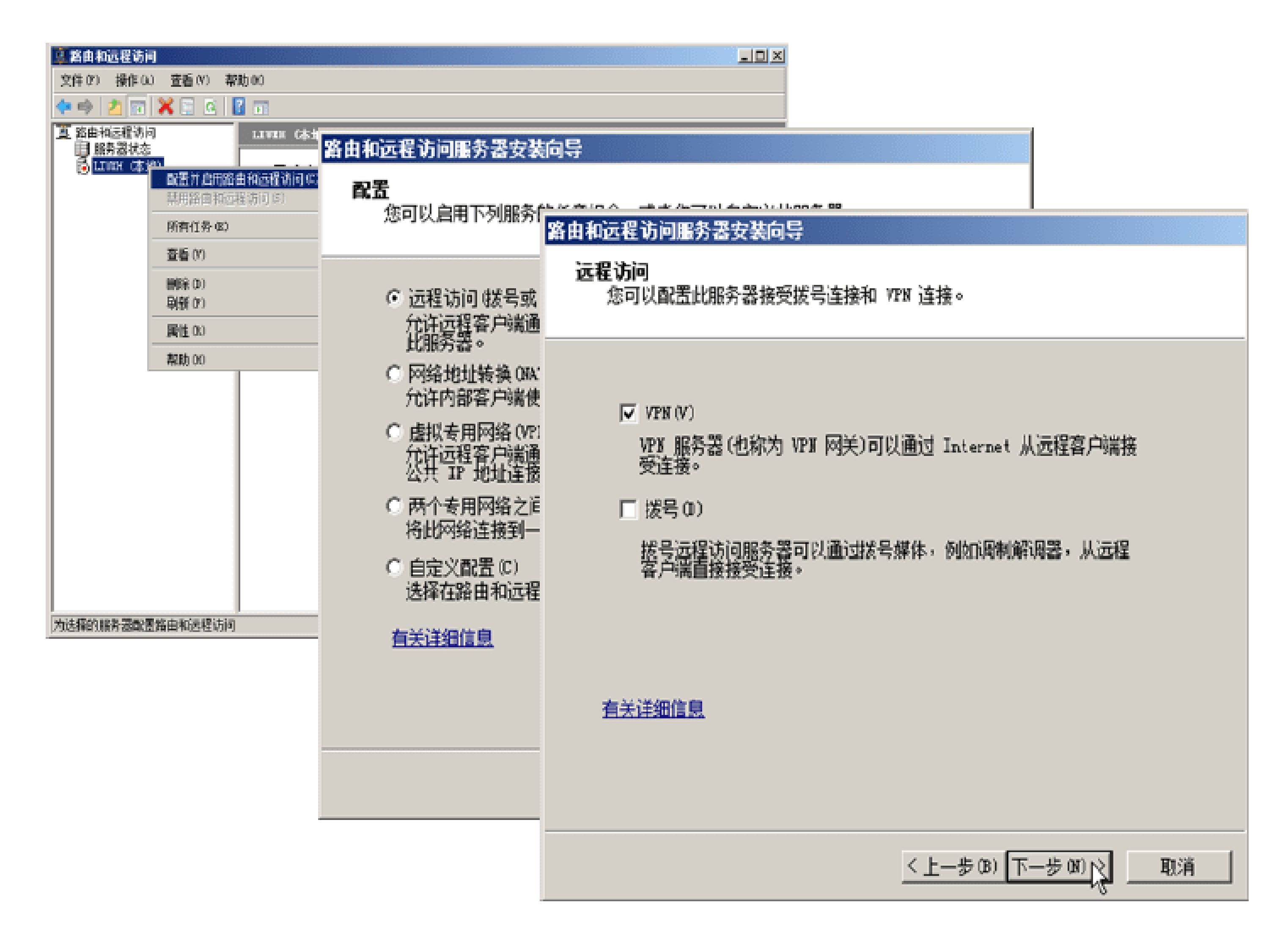


图 16.59　配置远程访问方法和类型

03 依次单击“下一步”按钮，设置 VPN 远程访问服务器的网络连接和 IP 地址分配方式，如图 16.60 所示。配置 VPN 远程访问服务器至少提供两块网卡，即一块连接 Internet，相应远程用户的访问，另一块用于连接内网。在“网络接口”列表中选择此服务连接到 Internet 的连接即可。管理员可以指定远程客户端获得 IP 地址的方式，如果本地网络中已经配置 DHCP 服务器，可以选择“自动”方式，客户端可以从 DHCP 服务器获得内网 IP 地址。否则，可以选择“来自一个指定的地址范围”单选按钮。

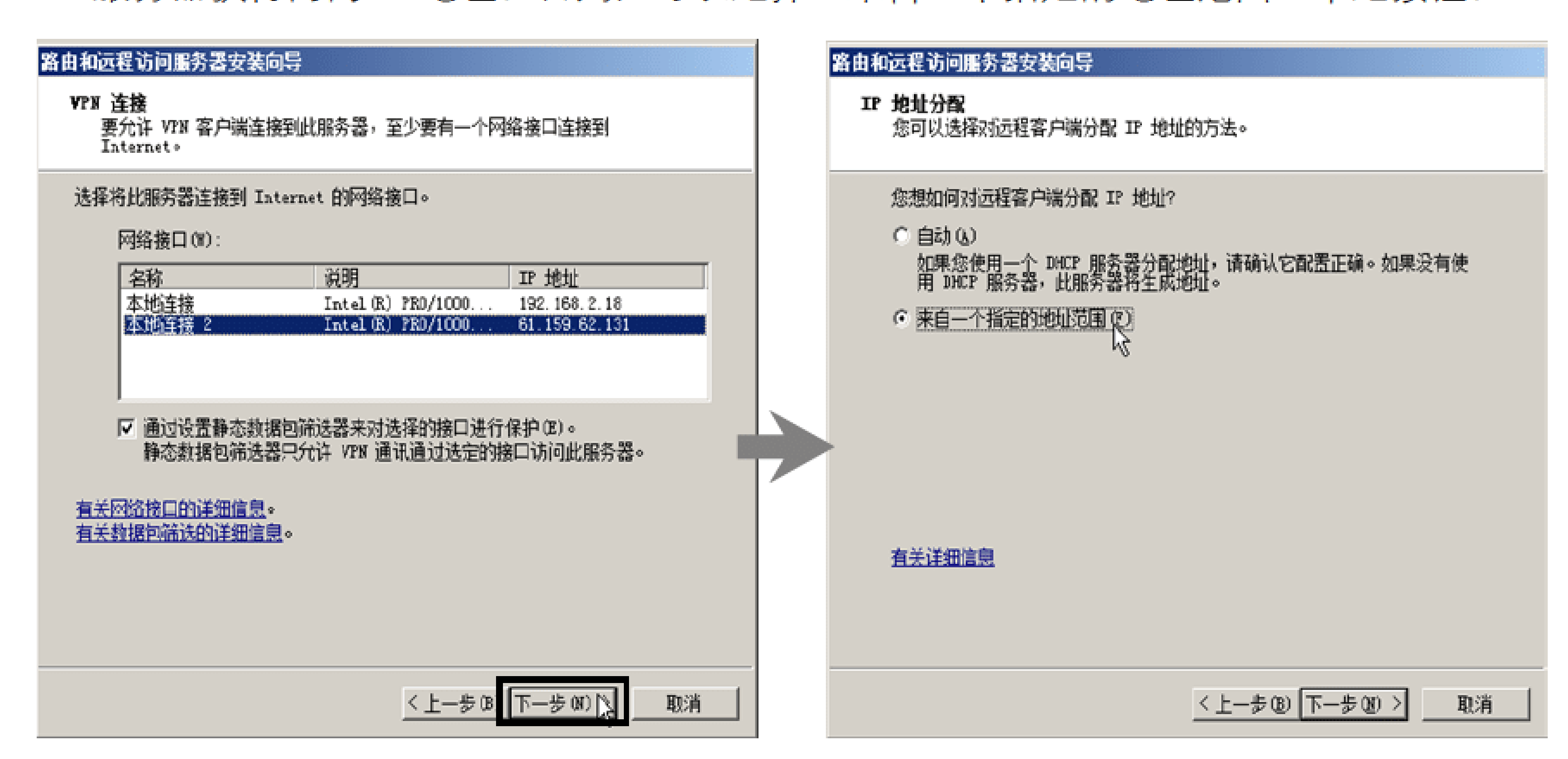


图 16.60　VPN 连接 IP 地址分配

04 单击“下一步”按钮，显示“管理多个远程访问服务器”对话框。如果计划在专用网络上安装多个 VPN 服务器、无线访问点或其他 RADIUS 客户端，添加 RADIUS 服务器非常有用。否则保留默认的“否，使用路由和远程访问来对连接请求进行身份验证”单选按钮即可。该选择将服务器配置为使用 Windows 身份验证、Windows 记账和本地存储的远程访问策略，在本地对连接请求进行身份验证。继续单击“下一步”按钮，即可完成 VPN 服务器配置，此时会提示用户在设置远程访问服务器以后，需要再指定 DHCP 服务器的 IP 地址。如图 16.61 所示。



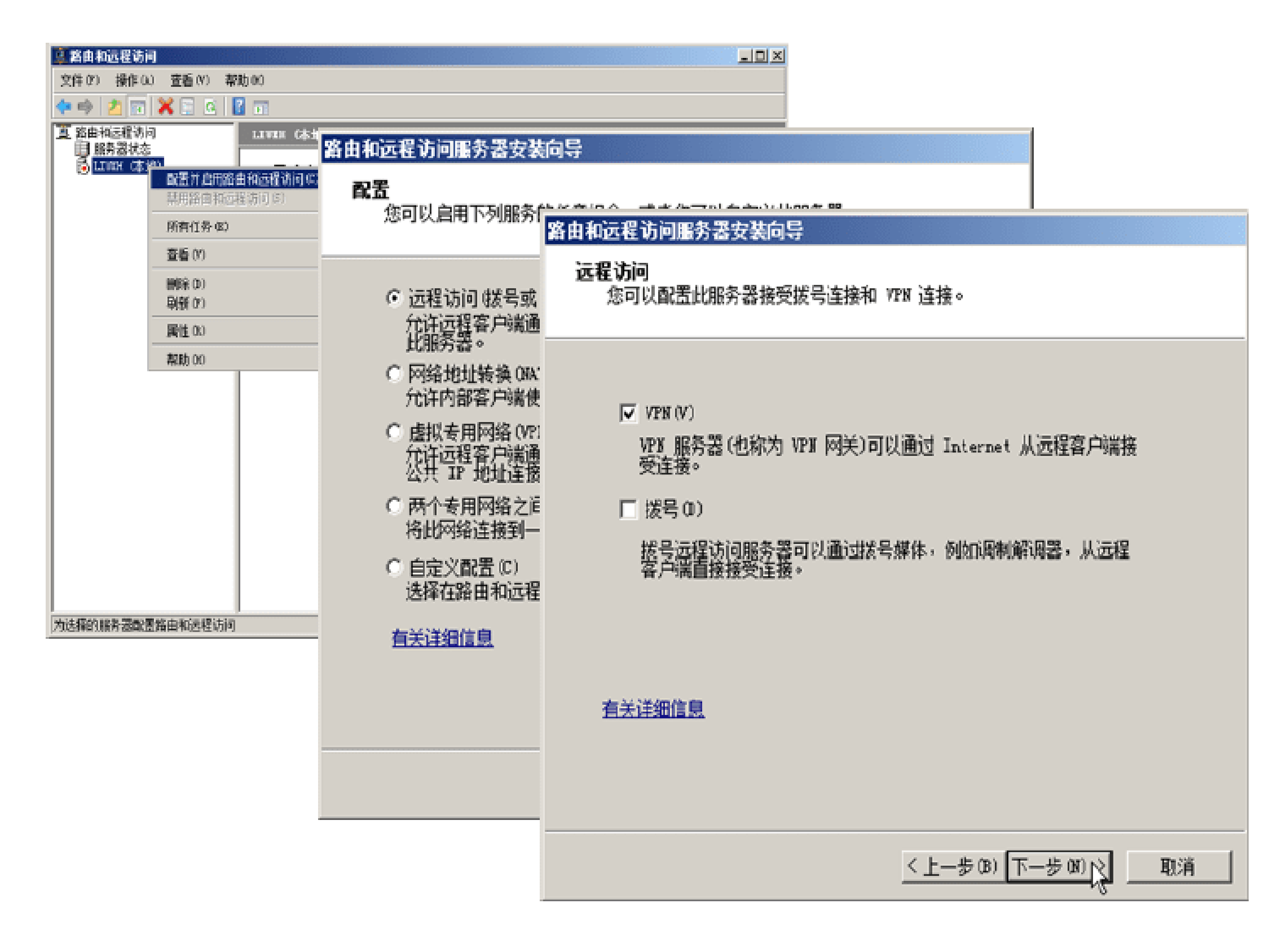


图 16.59 配置远程访问方法和类型

03 依次单击“下一步”按钮，设置 VPN 远程访问服务器的网络连接和 IP 地址分配方式，如图 16.60 所示。配置 VPN 远程访问服务器至少提供两块网卡，即一块连接 Internet，相应远程用户的访问，另一块用于连接内网。在“网络接口”列表中选择此服务连接到 Internet 的连接即可。管理员可以指定远程客户端获得 IP 地址的方式，如果本地网络中已经配置 DHCP 服务器，可以选择“自动”方式，客户端可以从 DHCP 服务器获得内网 IP 地址。否则，可以选择“来自一个指定的地址范围”单选按钮。

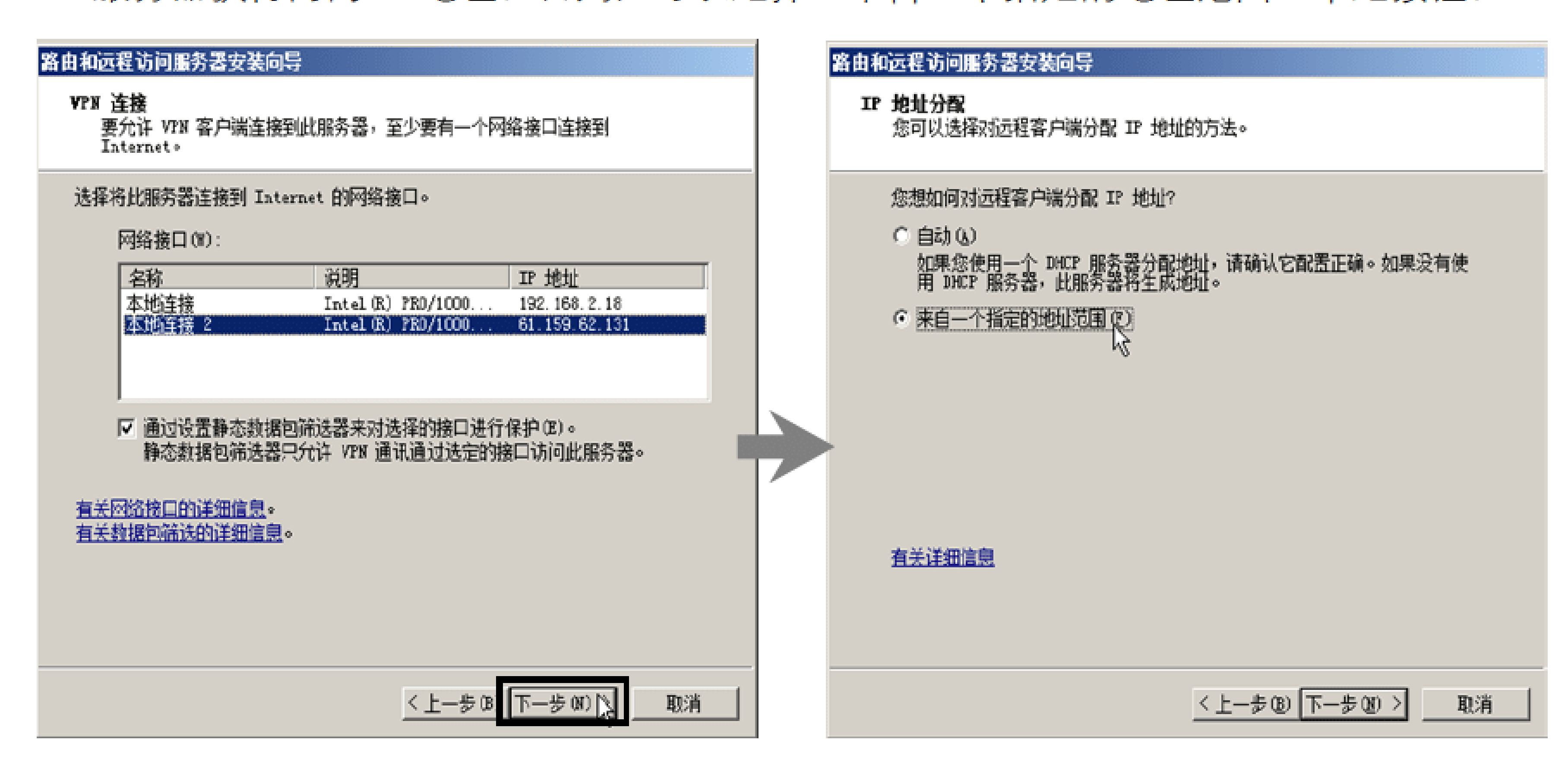


图 16.60 VPN 连接 IP 地址分配

04 单击“下一步”按钮，显示“管理多个远程访问服务器”对话框。如果计划在专用网络上安装多个 VPN 服务器、无线访问点或其他 RADIUS 客户端，添加 RADIUS 服务器非常有用。否则保留默认的“否，使用路由和远程访问来对连接请求进行身份验证”单选按钮即可。该选择将服务器配置为使用 Windows 身份验证、Windows 记账和本地存储的远程访问策略，在本地对连接请求进行身份验证。继续单击“下一步”按钮，即可完成 VPN 服务器配置，此时会提示用户在设置远程访问服务器以后，需要再指定 DHCP 服务器的 IP 地址。如图 16.61 所示。



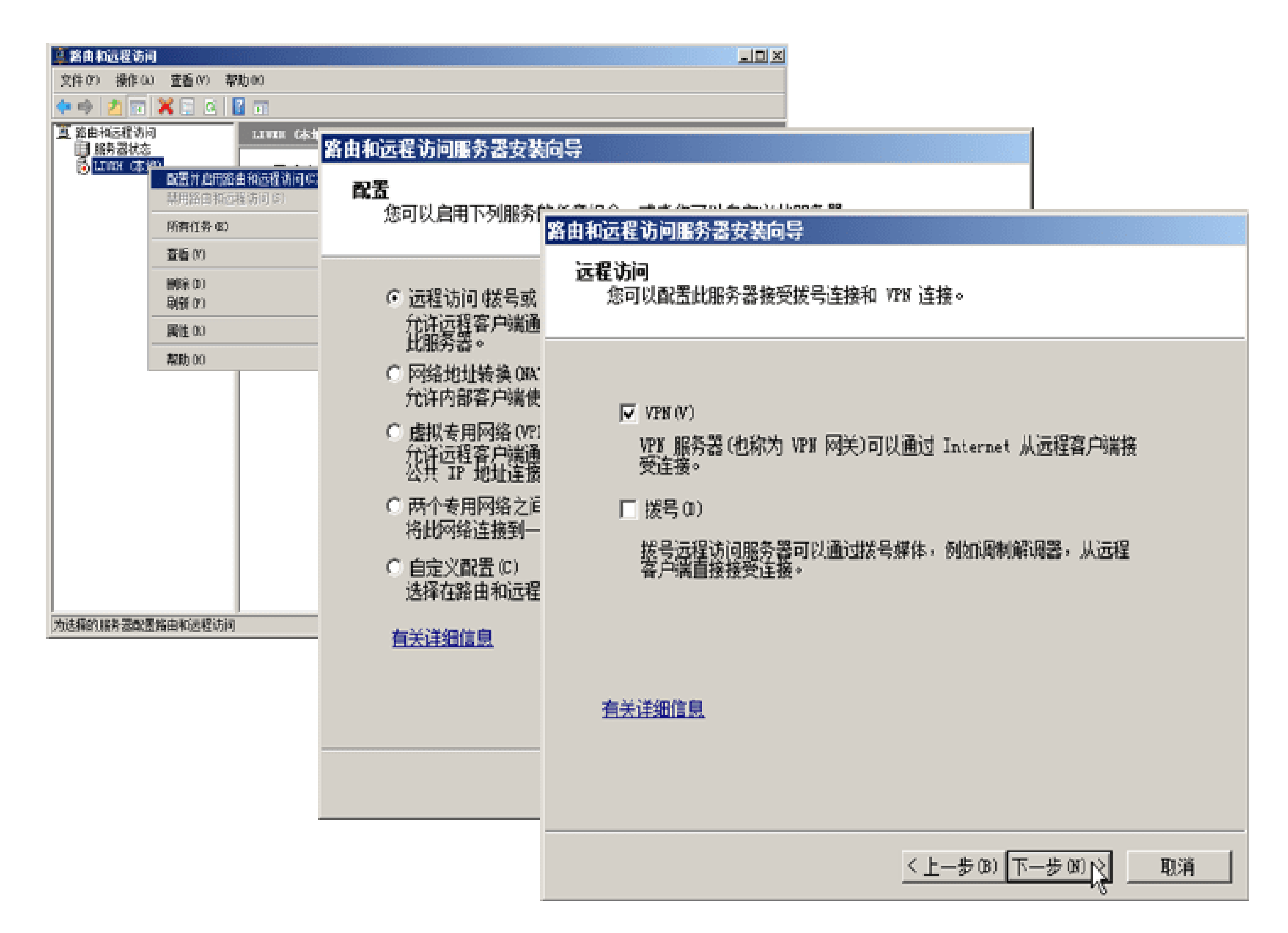


图 16.59　配置远程访问方法和类型

03 依次单击“下一步”按钮，设置 VPN 远程访问服务器的网络连接和 IP 地址分配方式，如图 16.60 所示。配置 VPN 远程访问服务器至少提供两块网卡，即一块连接 Internet，相应远程用户的访问，另一块用于连接内网。在“网络接口”列表中选择此服务连接到 Internet 的连接即可。管理员可以指定远程客户端获得 IP 地址的方式，如果本地网络中已经配置 DHCP 服务器，可以选择“自动”方式，客户端可以从 DHCP 服务器获得内网 IP 地址。否则，可以选择“来自一个指定的地址范围”单选按钮。

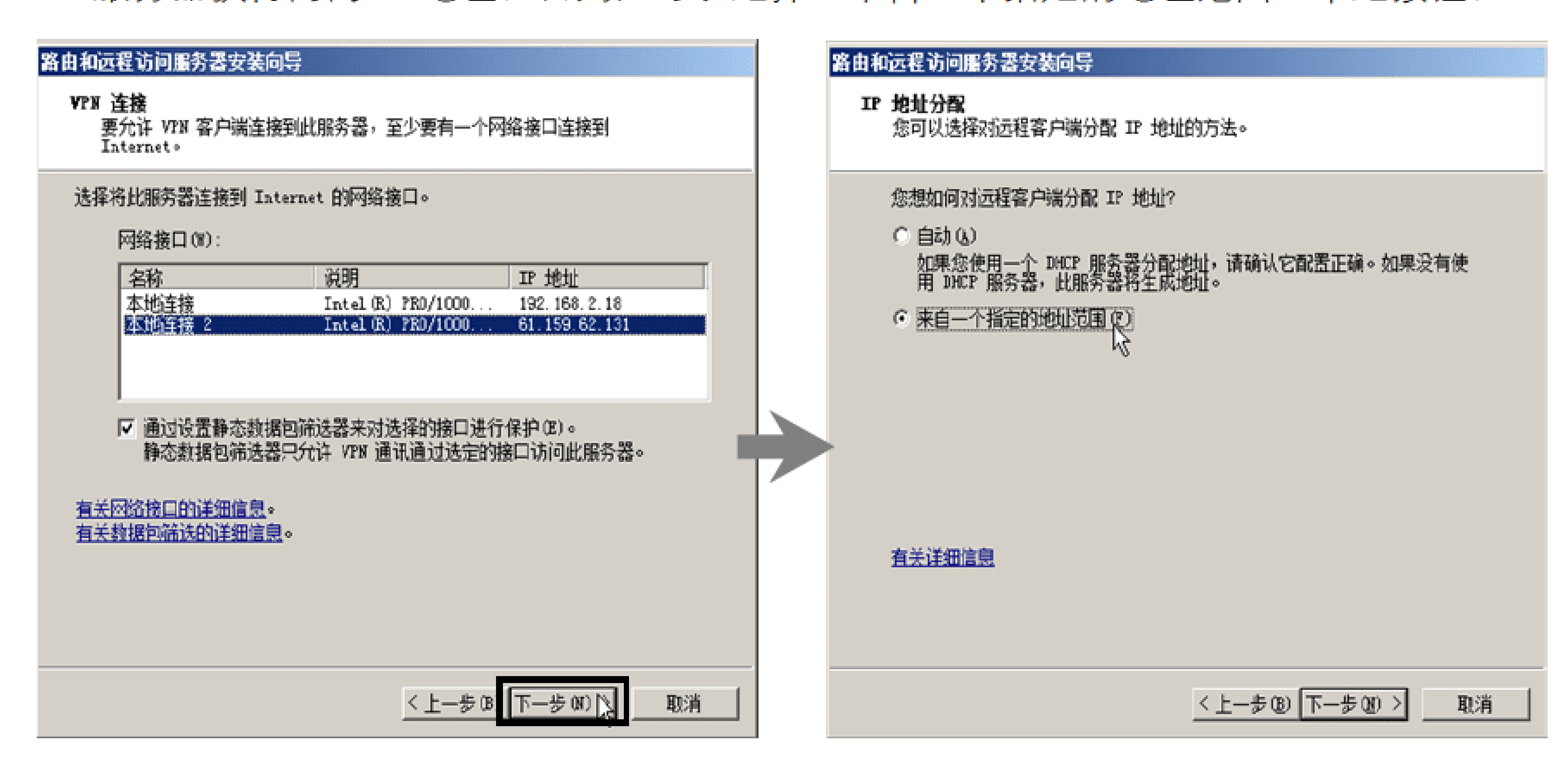


图 16.60　VPN 连接 IP 地址分配

04 单击“下一步”按钮，显示“管理多个远程访问服务器”对话框。如果计划在专用网络上安装多个 VPN 服务器、无线访问点或其他 RADIUS 客户端，添加 RADIUS 服务器非常有用。否则保留默认的“否，使用路由和远程访问来对连接请求进行身份验证”单选按钮即可。该选择将服务器配置为使用 Windows 身份验证、Windows 记账和本地存储的远程访问策略，在本地对连接请求进行身份验证。继续单击“下一步”按钮，即可完成 VPN 服务器配置，此时会提示用户在设置远程访问服务器以后，需要再指定 DHCP 服务器的 IP 地址。如图 16.61 所示。



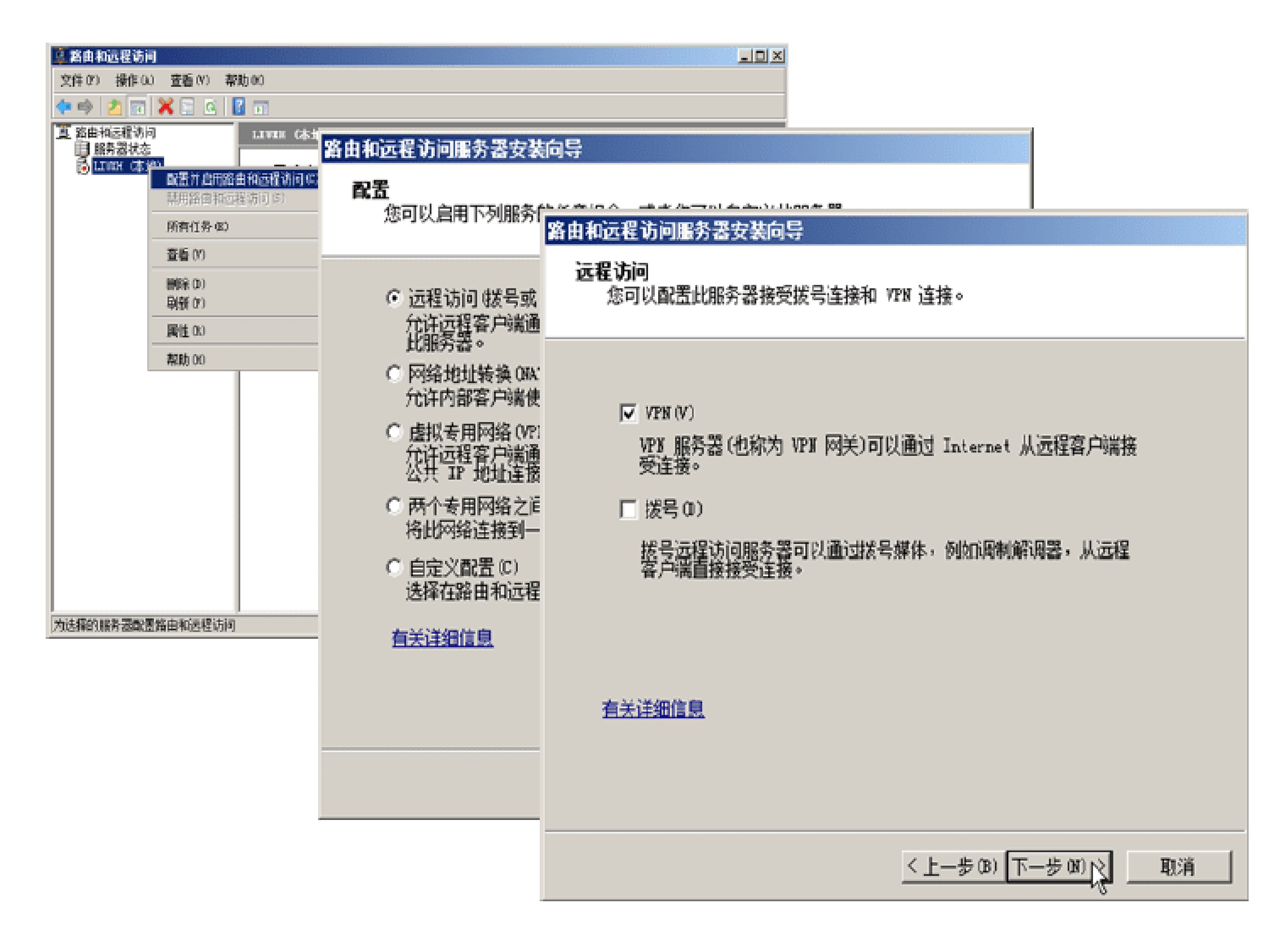


图 16.59　配置远程访问方法和类型

03 依次单击“下一步”按钮，设置 VPN 远程访问服务器的网络连接和 IP 地址分配方式，如图 16.60 所示。配置 VPN 远程访问服务器至少提供两块网卡，即一块连接 Internet，相应远程用户的访问，另一块用于连接内网。在“网络接口”列表中选择此服务连接到 Internet 的连接即可。管理员可以指定远程客户端获得 IP 地址的方式，如果本地网络中已经配置 DHCP 服务器，可以选择“自动”方式，客户端可以从 DHCP 服务器获得内网 IP 地址。否则，可以选择“来自一个指定的地址范围”单选按钮。

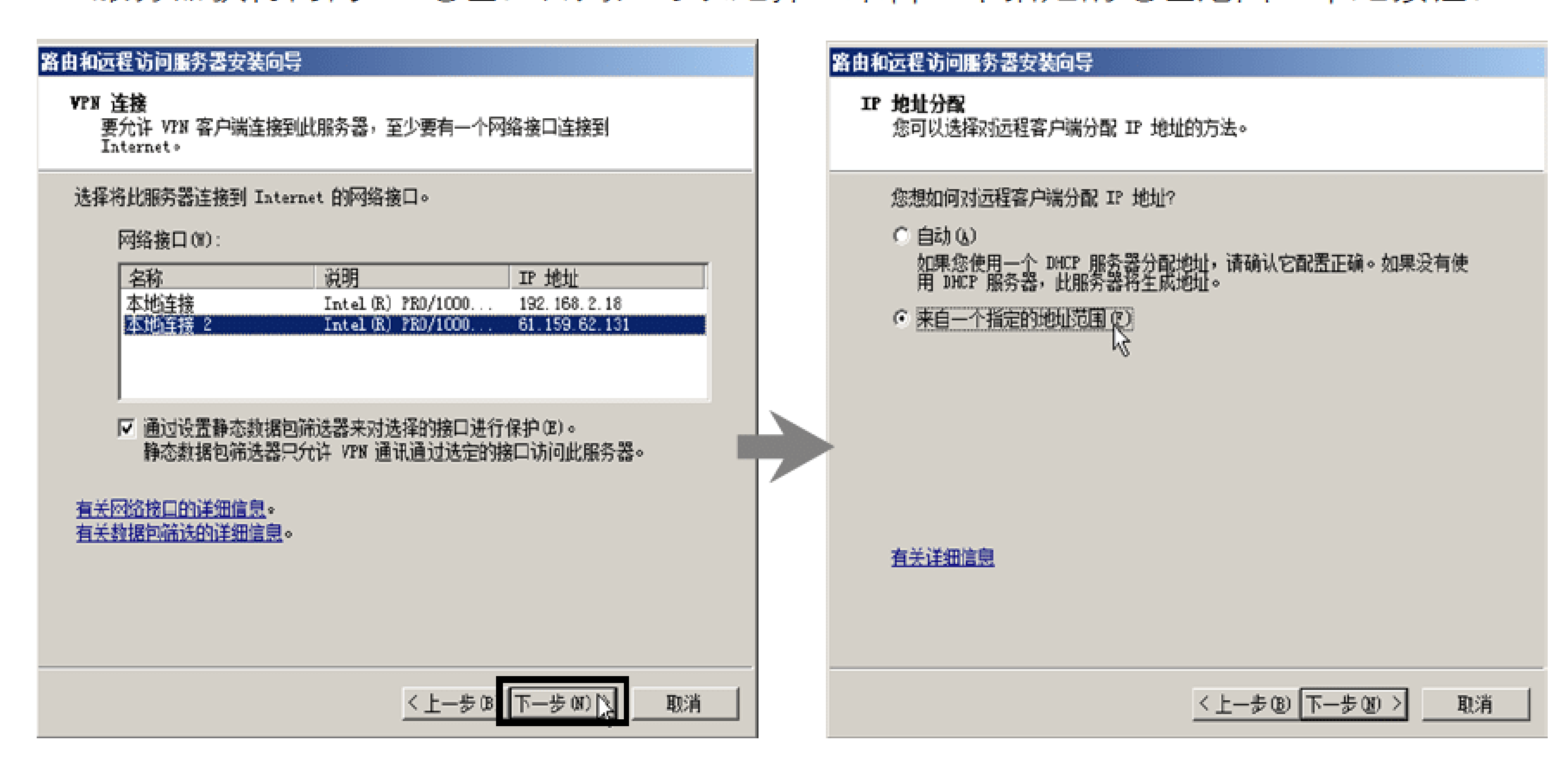


图 16.60　VPN 连接 IP 地址分配

04 单击“下一步”按钮，显示“管理多个远程访问服务器”对话框。如果计划在专用网络上安装多个 VPN 服务器、无线访问点或其他 RADIUS 客户端，添加 RADIUS 服务器非常有用。否则保留默认的“否，使用路由和远程访问来对连接请求进行身份验证”单选按钮即可。该选择将服务器配置为使用 Windows 身份验证、Windows 记账和本地存储的远程访问策略，在本地对连接请求进行身份验证。继续单击“下一步”按钮，即可完成 VPN 服务器配置，此时会提示用户在设置远程访问服务器以后，需要再指定 DHCP 服务器的 IP 地址。如图 16.61 所示。



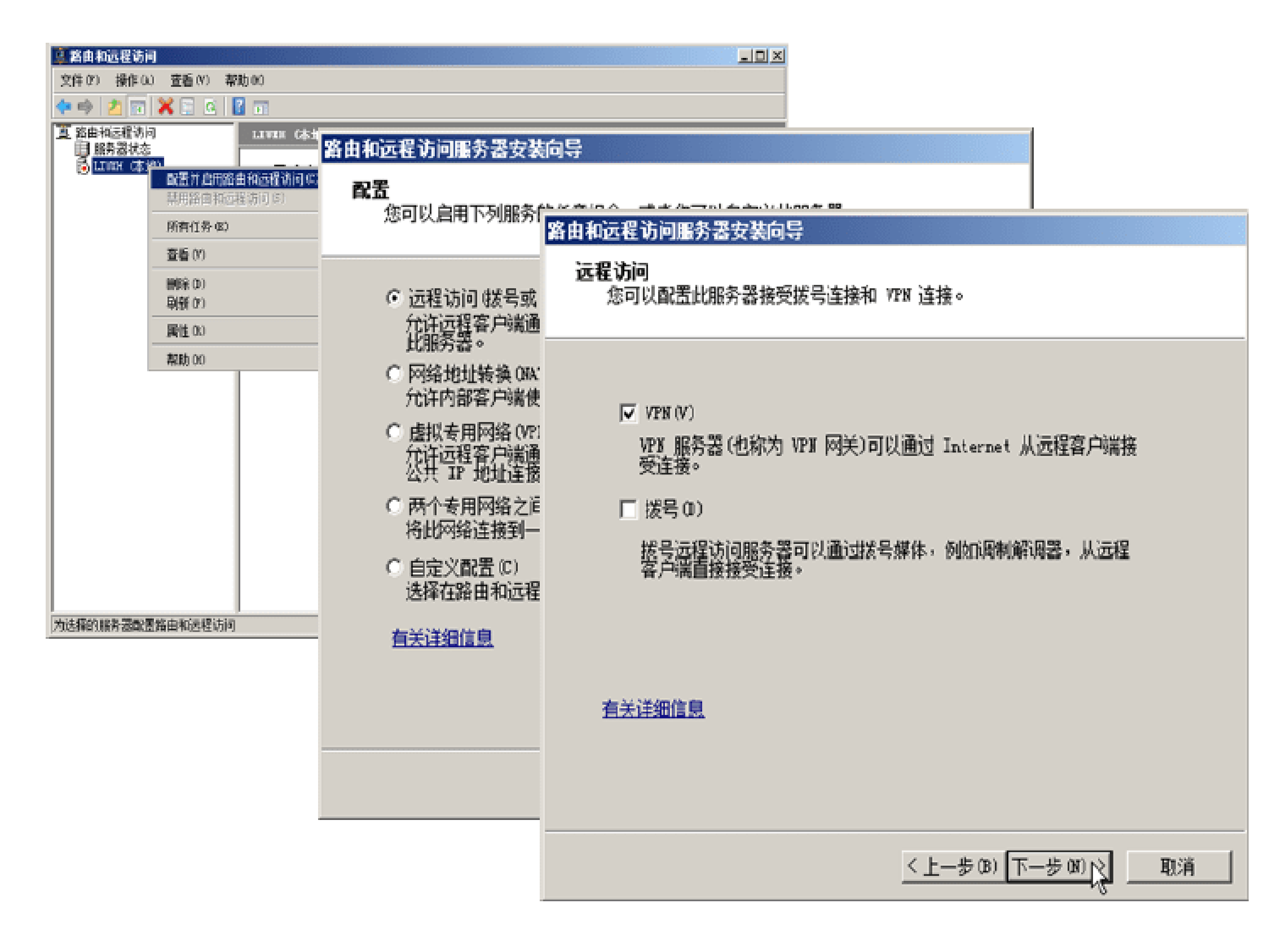


图 16.59　配置远程访问方法和类型

03 依次单击“下一步”按钮，设置 VPN 远程访问服务器的网络连接和 IP 地址分配方式，如图 16.60 所示。配置 VPN 远程访问服务器至少提供两块网卡，即一块连接 Internet，相应远程用户的访问，另一块用于连接内网。在“网络接口”列表中选择此服务连接到 Internet 的连接即可。管理员可以指定远程客户端获得 IP 地址的方式，如果本地网络中已经配置 DHCP 服务器，可以选择“自动”方式，客户端可以从 DHCP 服务器获得内网 IP 地址。否则，可以选择“来自一个指定的地址范围”单选按钮。

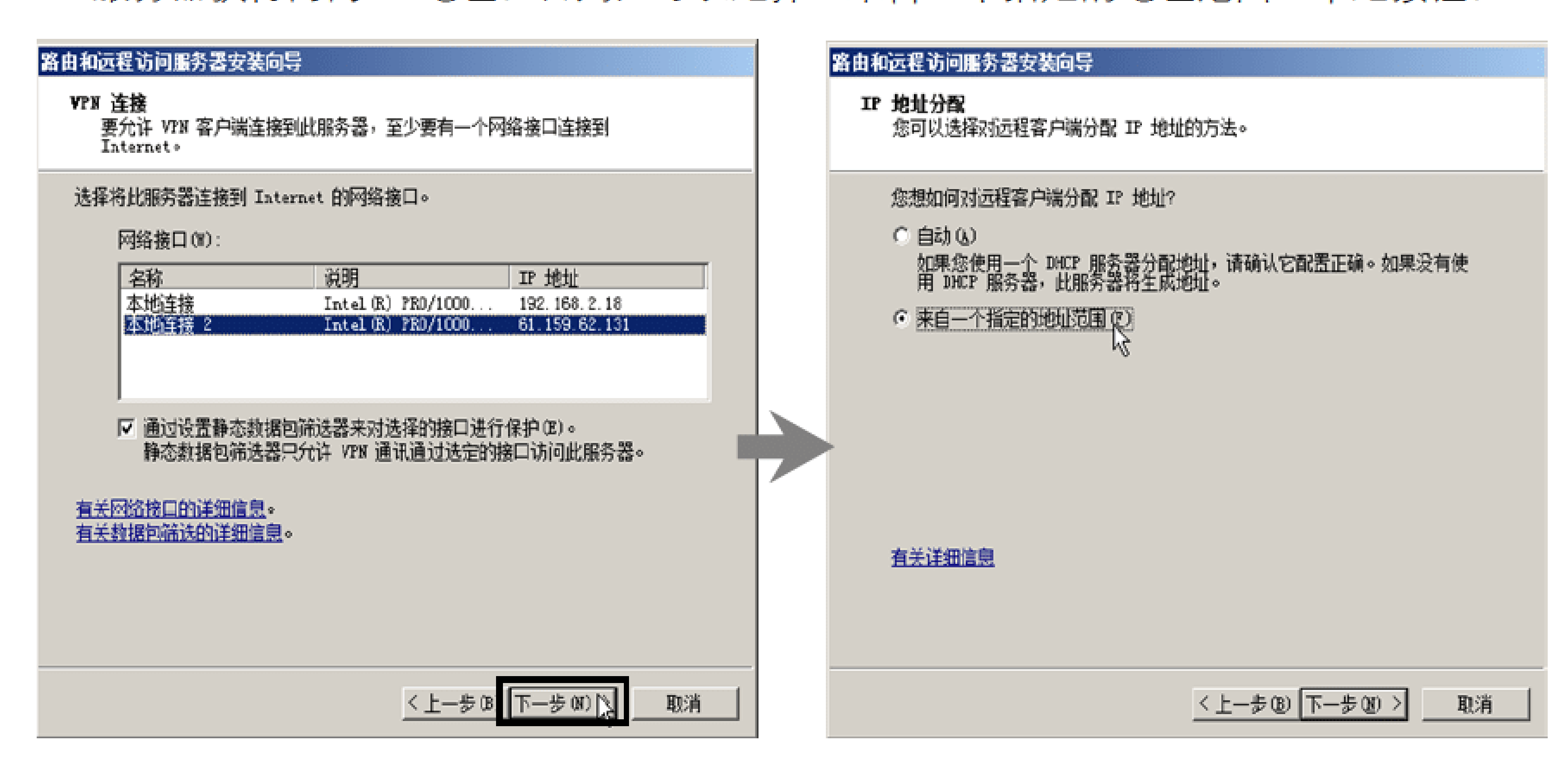


图 16.60　VPN 连接 IP 地址分配

04 单击“下一步”按钮，显示“管理多个远程访问服务器”对话框。如果计划在专用网络上安装多个 VPN 服务器、无线访问点或其他 RADIUS 客户端，添加 RADIUS 服务器非常有用。否则保留默认的“否，使用路由和远程访问来对连接请求进行身份验证”单选按钮即可。该选择将服务器配置为使用 Windows 身份验证、Windows 记账和本地存储的远程访问策略，在本地对连接请求进行身份验证。继续单击“下一步”按钮，即可完成 VPN 服务器配置，此时会提示用户在设置远程访问服务器以后，需要再指定 DHCP 服务器的 IP 地址。如图 16.61 所示。



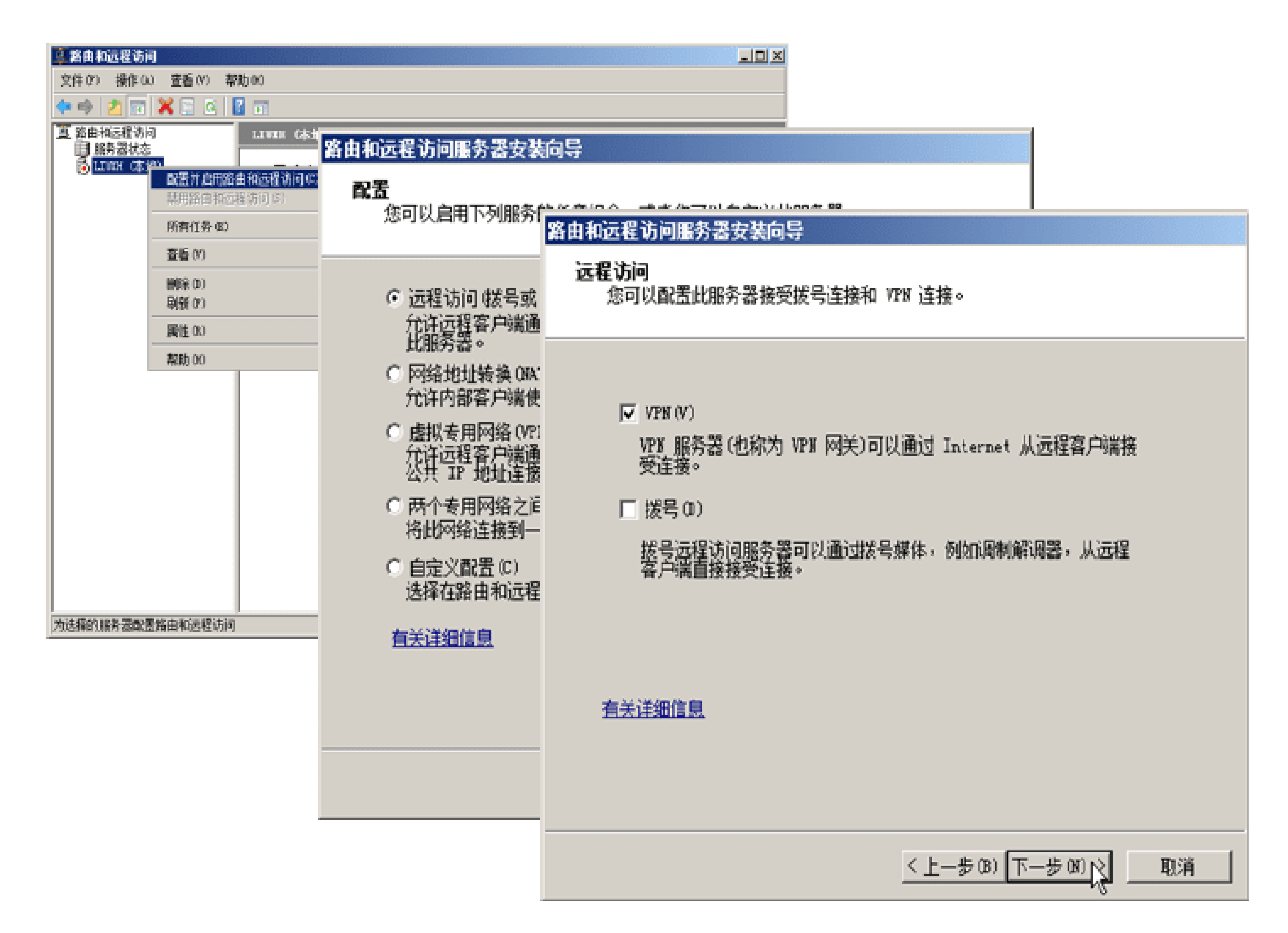


图 16.59　配置远程访问方法和类型

03 依次单击“下一步”按钮，设置 VPN 远程访问服务器的网络连接和 IP 地址分配方式，如图 16.60 所示。配置 VPN 远程访问服务器至少提供两块网卡，即一块连接 Internet，相应远程用户的访问，另一块用于连接内网。在“网络接口”列表中选择此服务连接到 Internet 的连接即可。管理员可以指定远程客户端获得 IP 地址的方式，如果本地网络中已经配置 DHCP 服务器，可以选择“自动”方式，客户端可以从 DHCP 服务器获得内网 IP 地址。否则，可以选择“来自一个指定的地址范围”单选按钮。

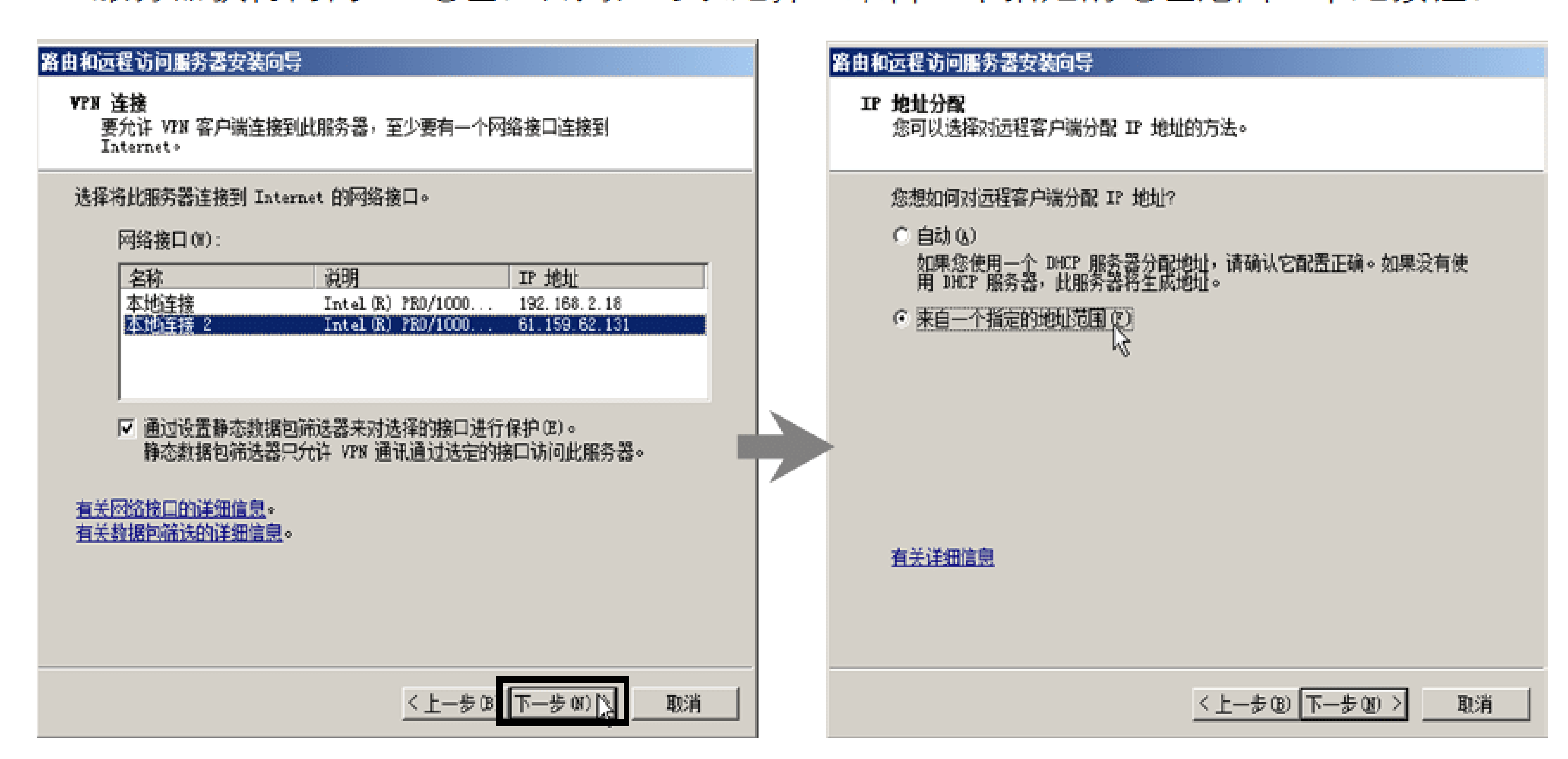


图 16.60　VPN 连接 IP 地址分配

04 单击“下一步”按钮，显示“管理多个远程访问服务器”对话框。如果计划在专用网络上安装多个 VPN 服务器、无线访问点或其他 RADIUS 客户端，添加 RADIUS 服务器非常有用。否则保留默认的“否，使用路由和远程访问来对连接请求进行身份验证”单选按钮即可。该选择将服务器配置为使用 Windows 身份验证、Windows 记账和本地存储的远程访问策略，在本地对连接请求进行身份验证。继续单击“下一步”按钮，即可完成 VPN 服务器配置，此时会提示用户在设置远程访问服务器以后，需要再指定 DHCP 服务器的 IP 地址。如图 16.61 所示。

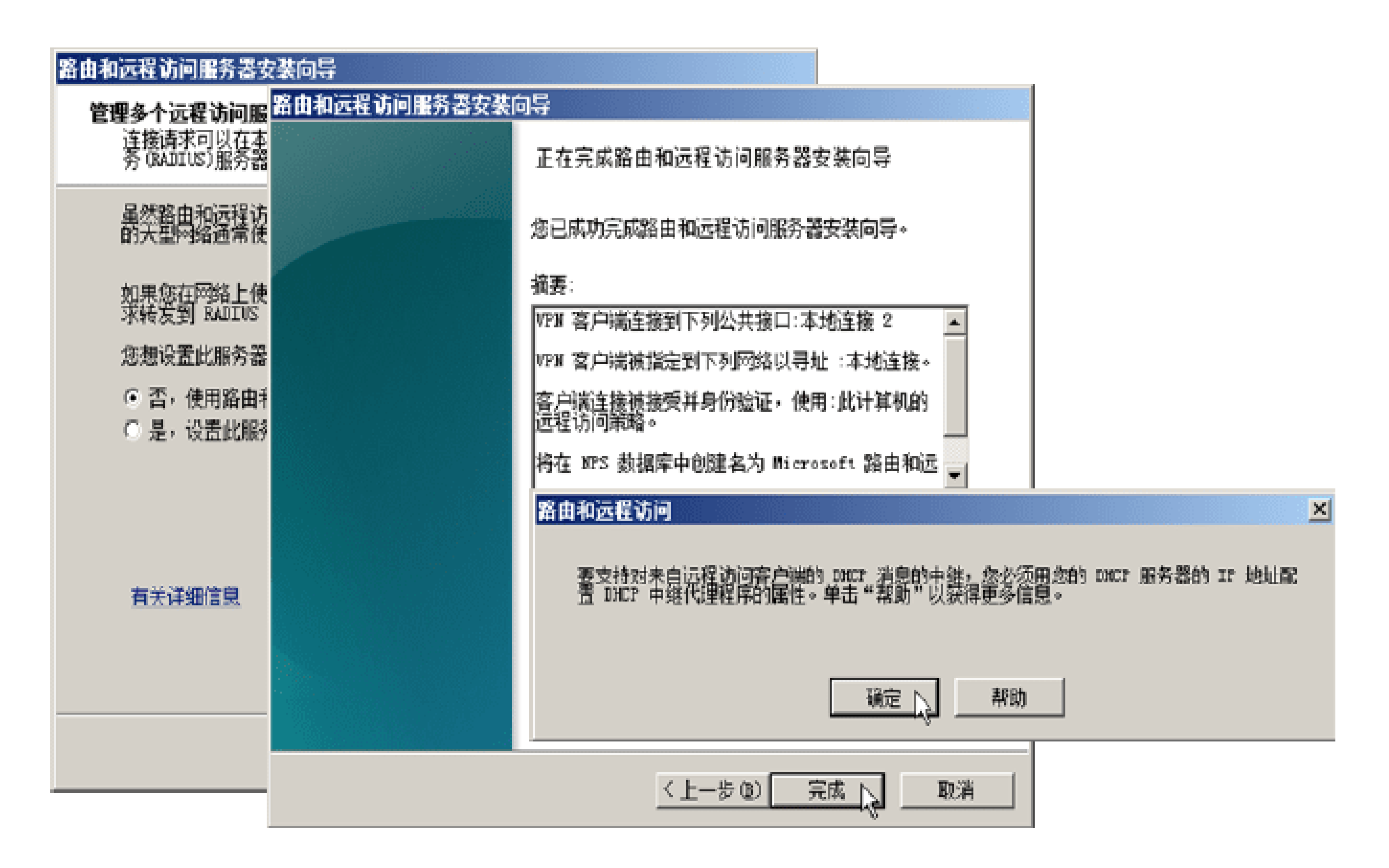


图 16.61　完成 VPN 远程访问服务器的配置

2. 赋予用户拨入权限

默认状态下，VPN 服务器禁止所有用户拨入，管理员需要对特定用户帐户赋予访问权限，否则将无法正常使用。

01 依次单击“开始”→“管理工具”→“Active Directory 用户和计算机”，打开“Active Directory 用户和计算机”窗口。选择想要设置拨入权限的用户帐户，右击并选择快捷菜单中的“属性”选项，打开“用户 属性”对话框，单击“拨入”选项卡，在“网络访问权限”选项区域中选择“允许访问”单选按钮。如图 16.62 所示。

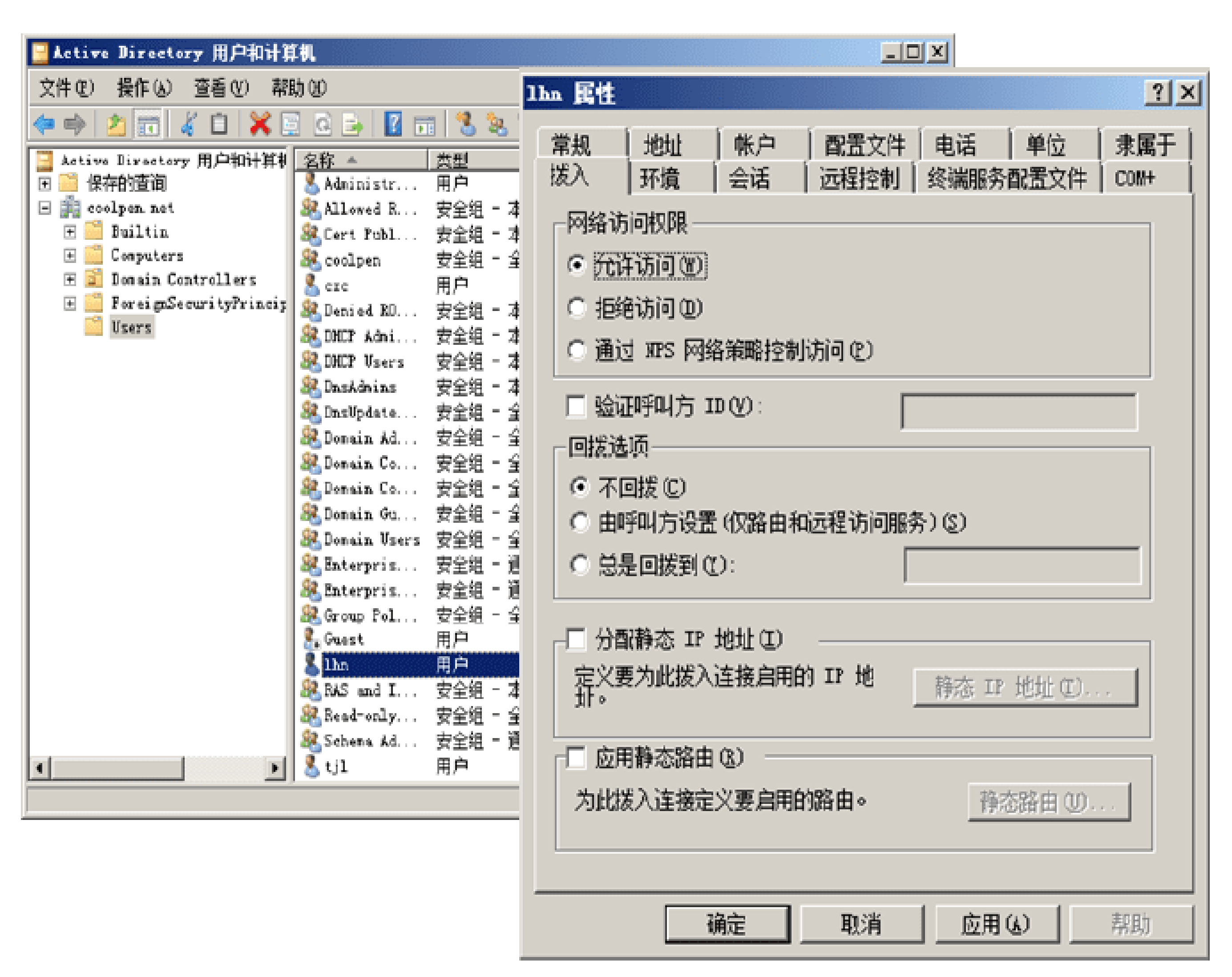


图 16.62　赋予用户拨入权限

02 单击“确定”按钮保存即可。按照同样步骤，可继续为其他用户启用拨入功能。



提示　“通过 NPS 网络策略控制访问”是要求 VPN 客户端，必须通过本地服务器或当前网络中的网络策略服务器的身份验证，才可以拨入。没有配置 NPS 的用户，直接选择“允许拨入”单选按钮即可。



3. 配置 RAIDUS 身份验证

VPN 服务器配置完毕之后，应确保其使用的身份验证方法为可扩展的身份验证协议或 Microsoft 加密身份验证版本 2。

01 在“路由和远程访问”控制台中，右击 VPN 服务器名，选择快捷菜单中的“属性”选项，打开服务器属性对话框。选择“安全”选项卡，确认在“身份验证提供程序”下拉列表中选择“RADIUS 身份验证”选项。单击“身份验证方法”按钮，显示“身份验证方法”对话框，确保已选中“可扩展的身份验证协议”或“Microsoft 加密身份验证版本 2”复选框。如图 16.63 所示。

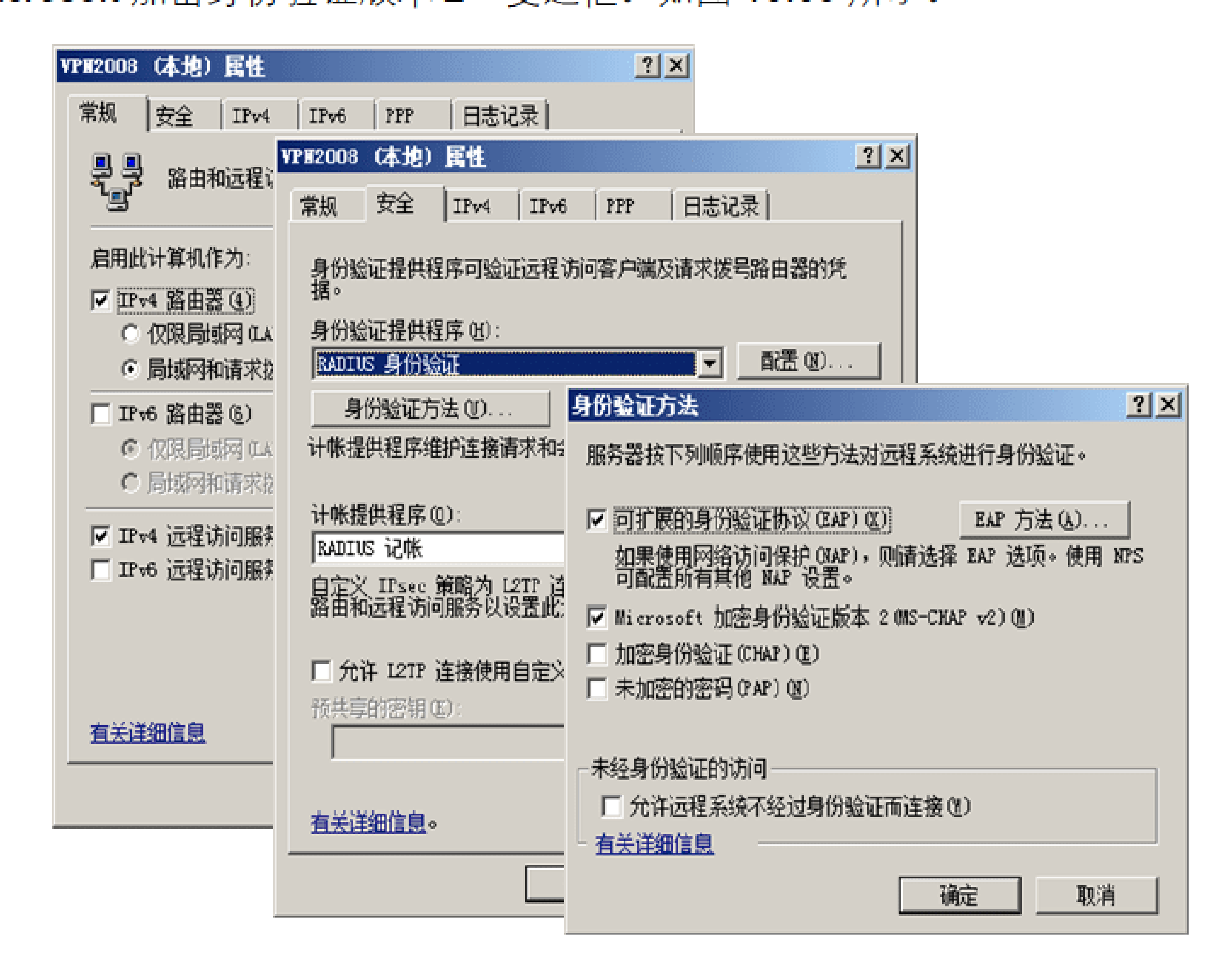


图 16.63　配置 RAIDUS 身份验证

02 依次单击“确定”按钮，保存并返回“路由和远程访问”窗口。

16.6.2　配置 NPS

网络访问策略服务器负责制定健康策略，对远程拨入的计算机进行检查，如果远程计算机符合策略要求就允许访问，否则就会访问受限。通常情况下，用户需要对现有 NPS 进行如下配置：

- 申请计算机验证证书；
- 配置网络访问策略；
- 配置系统健康验证器；
- 为 RADIUS 客户端配置 NPA 支持。

1. 申请计算机验证证书

在 NPS 服务器上打开控制台窗口，添加“证书”管理单元。不过，在选择帐户时应选择“计算机帐户”单选按钮。将证书管理单元添加到控制台中以后，展开“证书”，右击“个人”

并选择快捷菜单中的“所有任务”→“申请新证书”，启动“证书注册”向导，用来申请验证证书。依次单击“下一步”按钮，完成证书申请和注册。如图 16.64 所示。单击“完成”按钮，证书安装成功，并显示在“证书管理单元”中。

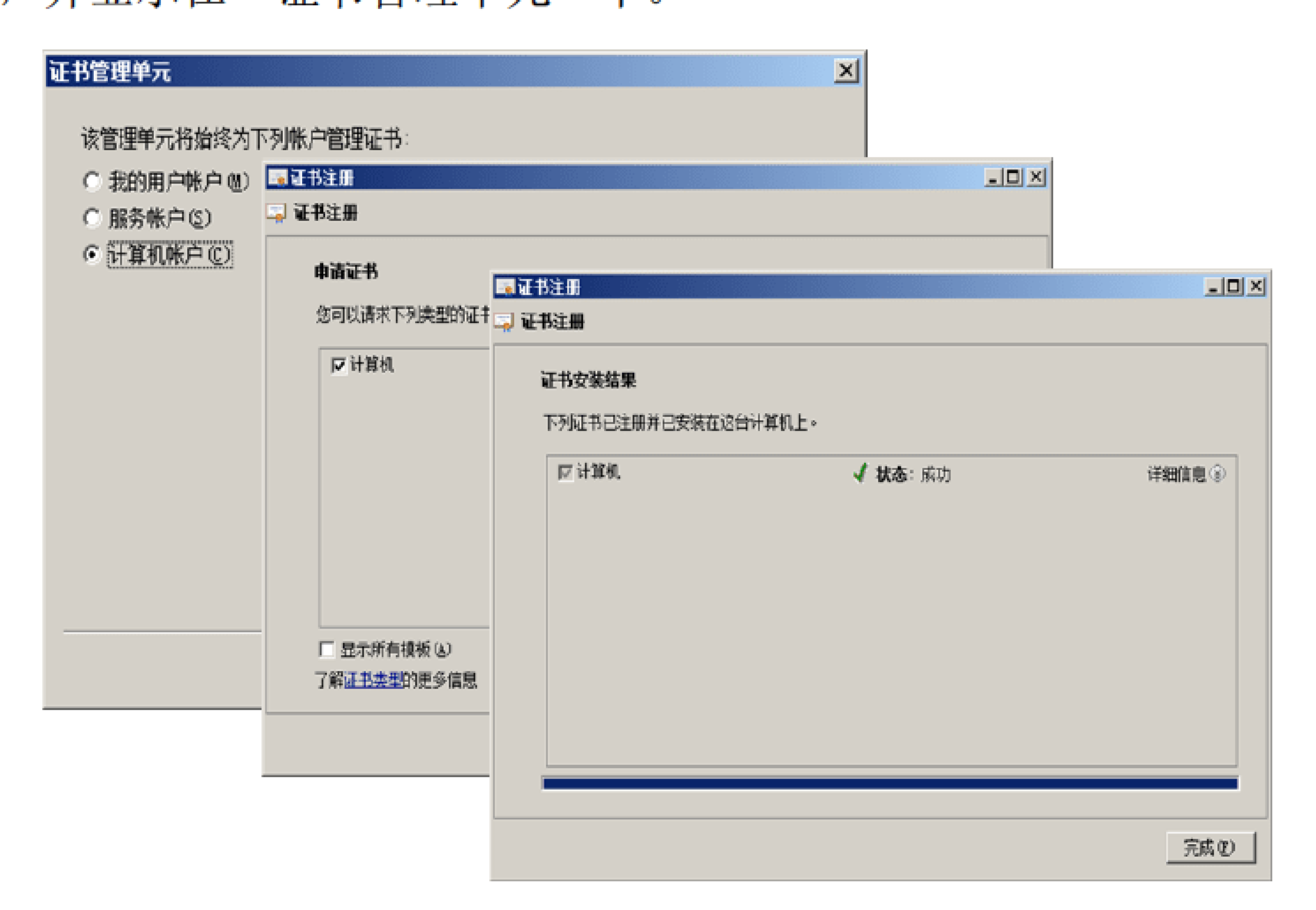


图 16.64　证书申请注册

提示　如果证书服务器上安装了“证书服务 Web 注册”功能，也可以通过 IE 浏览器来申请证书。

2. 配置网络访问策略

为 VPN 强制配置网络访问策略，可通过“配置 NAP”向导来完成。

01 依次选择“开始”→“管理工具”→“网络策略服务器”，打开“网络策略服务器”窗口，在右侧窗口的“标准配置”下拉列表中，选择“网络访问保护（NAP）”选项，单击“配置 NAP”链接，启动配置 NAP 向导。在“选择与 NAP 一起使用的网络连接方法”对话框中，从下拉列表中选择“虚拟专用网络（VPN）”选项，并在“策略名称”文本框中为该策略输入一个名称，如图 16.65 所示。

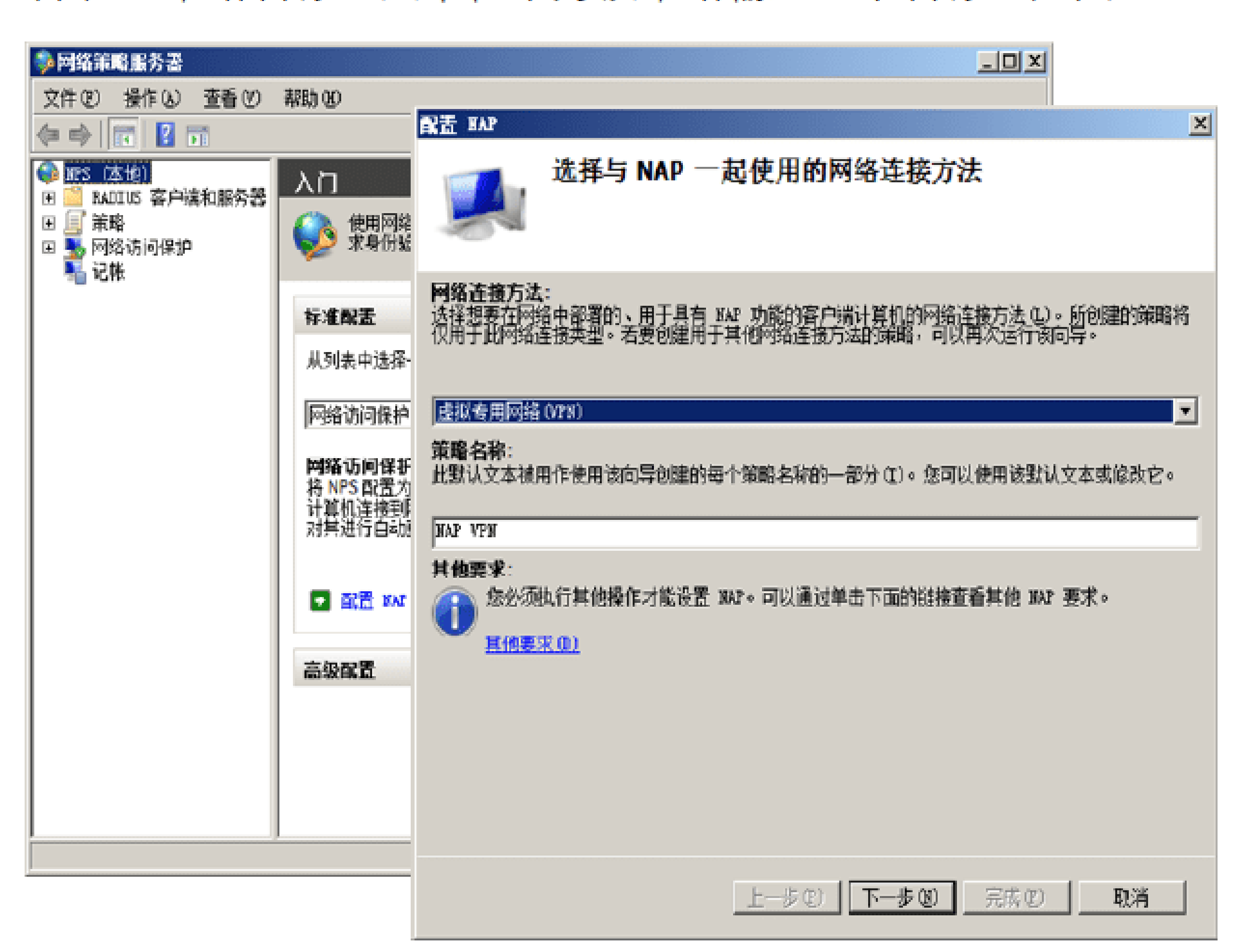


图 16.65　打开“选择与 NAP 一起使用的网络连接方法”对话框



02 单击“下一步”按钮，显示“指定 NAP 强制服务器运行 VPN 服务器”对话框，需要添加 RADIUS 客户端。在这里，RADIUS 服务器就是当前的 NPS 服务器，而 RADIUS 客户端则是 VPN 服务器。必须将 RADIUS 客户端添加到当前服务器，双方才能建立连接。单击“添加”按钮，显示“新建 RADIUS 客户端”对话框。在“友好名称”文本框中输入一个名称，在“地址(IP 或 DNS)”文本框中输入 VPN 服务器的 IP 地址，如果输入的是计算机名，应单击 “验证”按钮进行验证。在“共享机密”文本框中输入相应的密码。如图 16.66 所示。

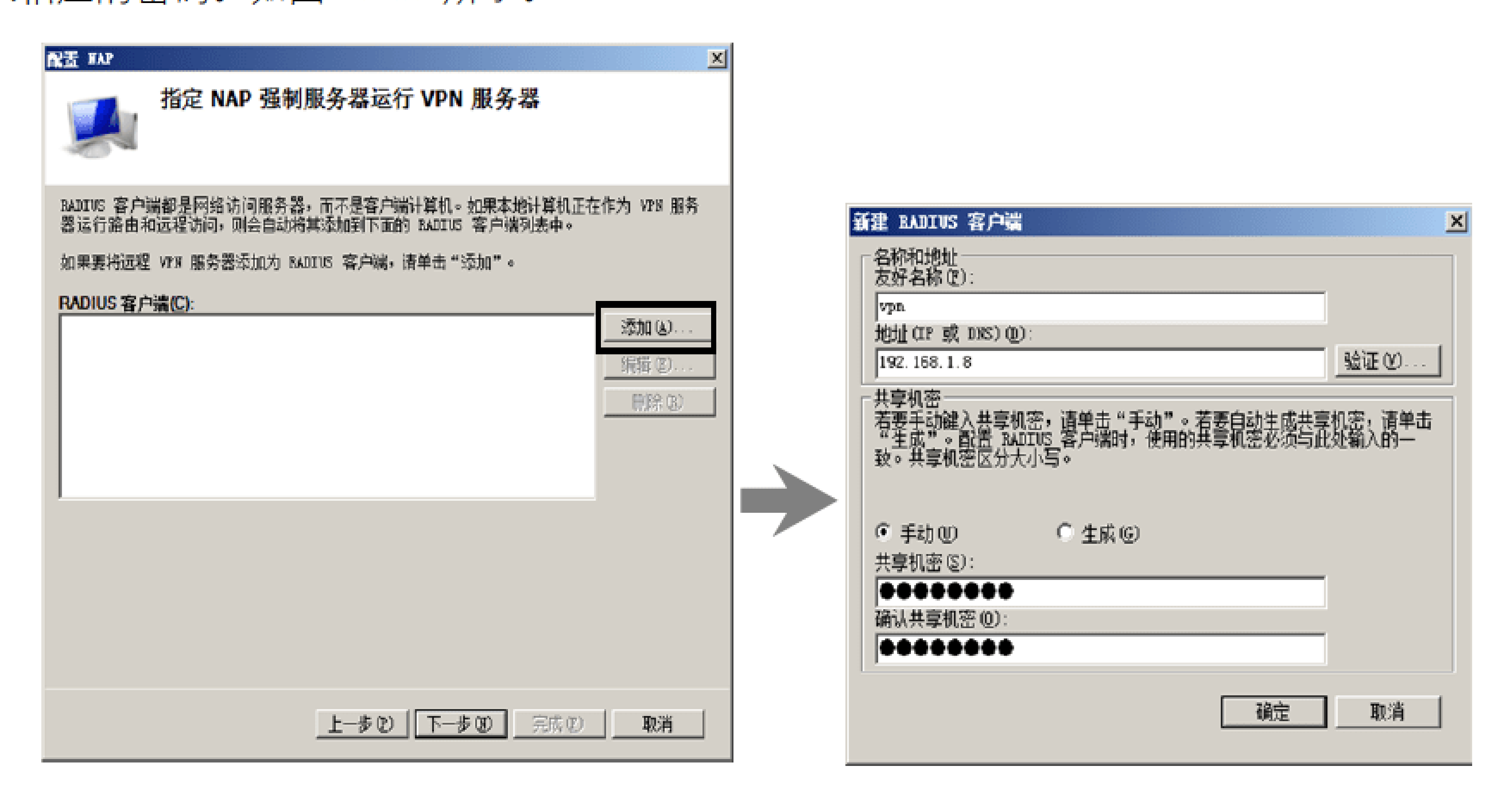


图 16.66　打开“新建 RADIUS 客户端”对话框

03 单击“下一步”按钮，显示如图 16.67 所示“配置用户组和计算机组”对话框，根据需要添加要允许或拒绝访问的计算机组或用户组。如果不选择，将对所有计算机组和用户组有效。

04 单击“下一步”按钮，显示如图 16.68 所示“配置身份验证方法”对话框，为受保护的可扩展身份验证协议（PEAP）选择 NPS 服务器证书，即前面所申请的证书。根据需要选择“安全密码（PEAP-MS-CHAP v2）”或者“智能卡或其他证书（EAP-TLS）”选项。需要注意的是，VPN 服务器、NPS 服务器和客户端必须设置为完全相同的身份验证方式，否则无法建立连接。

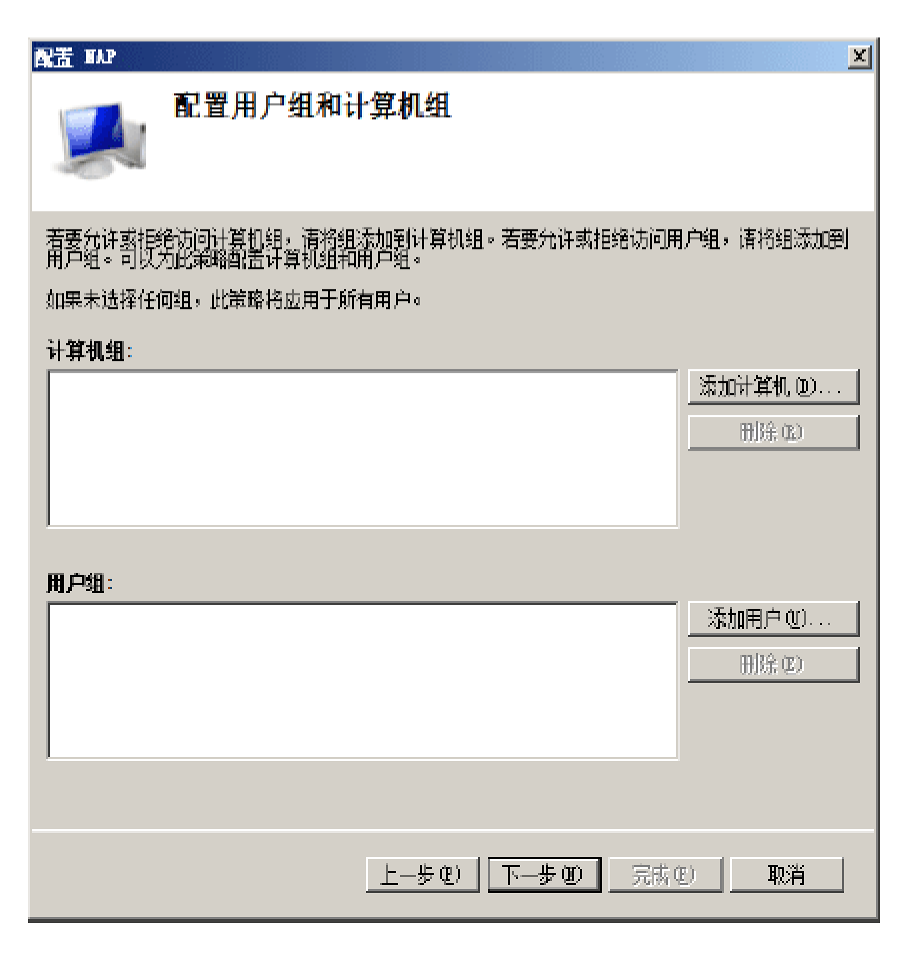




图 16.67　“配置用户组和计算机组”对话框

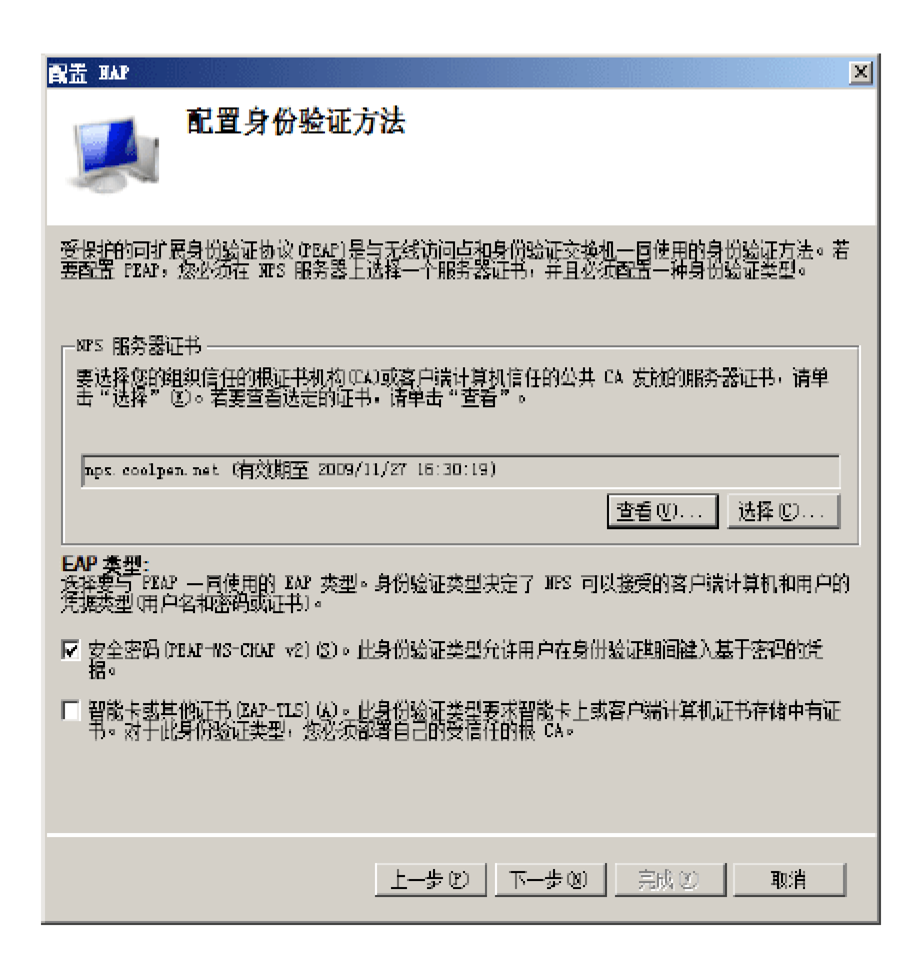


图 16.68　“配置身份验证方法”对话框

05 单击“下一步”按钮，显示“指定 NAP 更新服务器组和 URL”对话框。当客户端计算机未通过健康策略审查时，可以从更新服务器组中的服务器进行“补救”，通常为 WSUS 服务器、网络防病毒服务器等，

可使客户端安装系统更新或杀毒软件。单击“新建组”按钮，显示“新建更新服务器组”对话框，可以新建组并添加相应的服务器。单击“确定”按钮返回。当然，也可以不设置更新服务器组，例如仅检测网络防火墙开启状态等。如图 16.69 所示。

06 单击“下一步”按钮，显示如图 16.70 所示“定义 NAP 健康策略”对话框，选择 VPN 强制需要的系统健康验证器。默认选中“启用客户端计算机的自动更新”复选框，如果客户端计算机没有启用自动更新，会强制启用。由于客户端计算机安装的可能是不具有 NAP 功能的操作系统，因此，可选择“拒绝对不具有 NAP 功能的客户端计算机的完全网络访问权限。只允许访问受限网络。”单选按钮，使其只能访问受限网络。

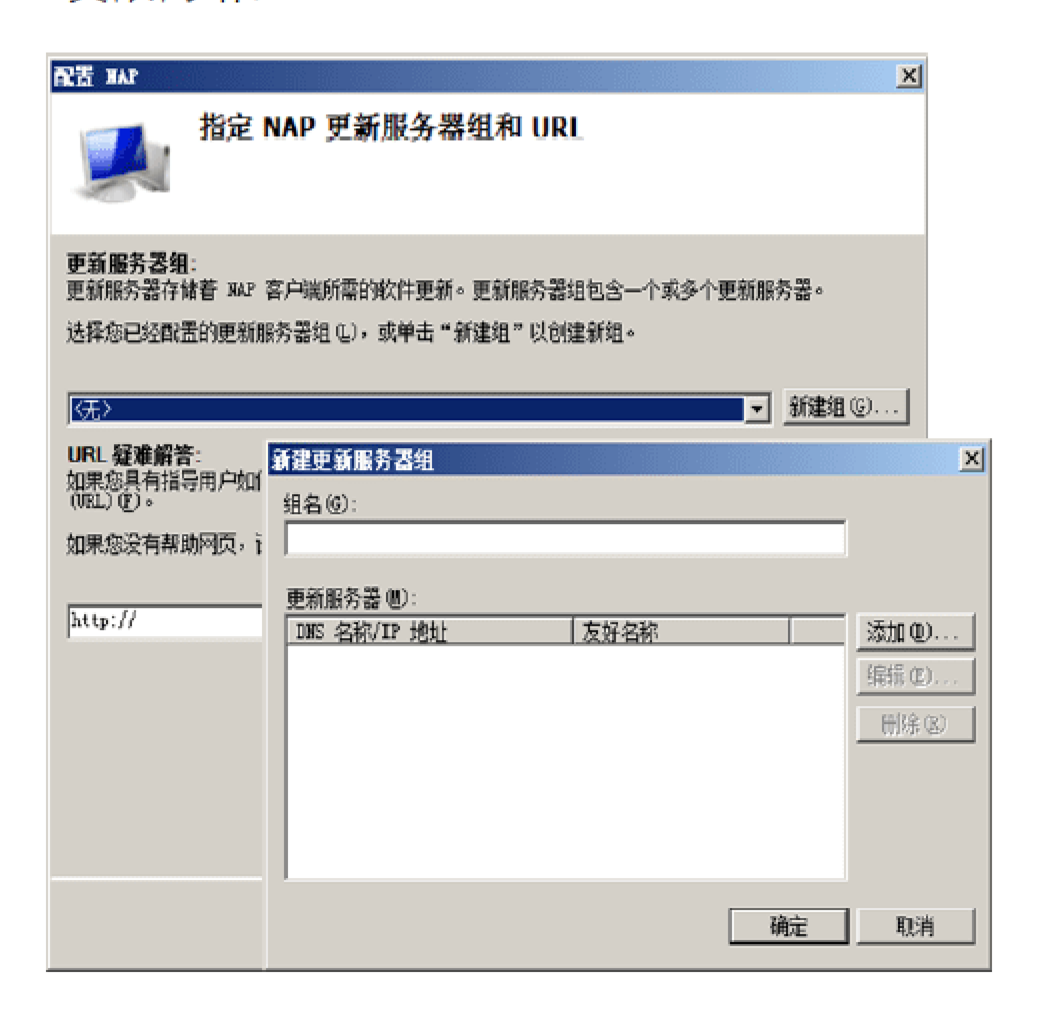


图 16.69　指定 NAP 更新服务器组和 URL

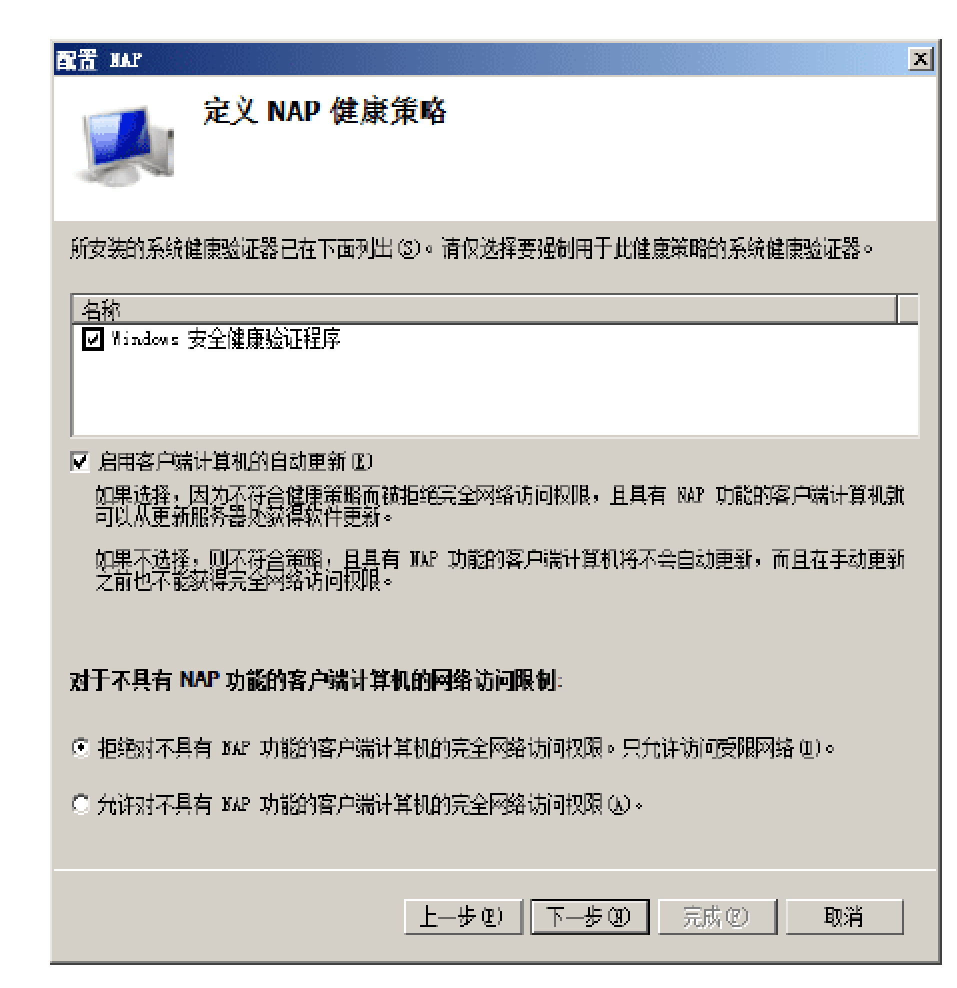


图 16.70　“定义 NAP 健康策略”对话框

07 单击“下一步”按钮，显示前面所做的配置。单击“完成”按钮配置完成，并返回“网络策略服务器”窗口。

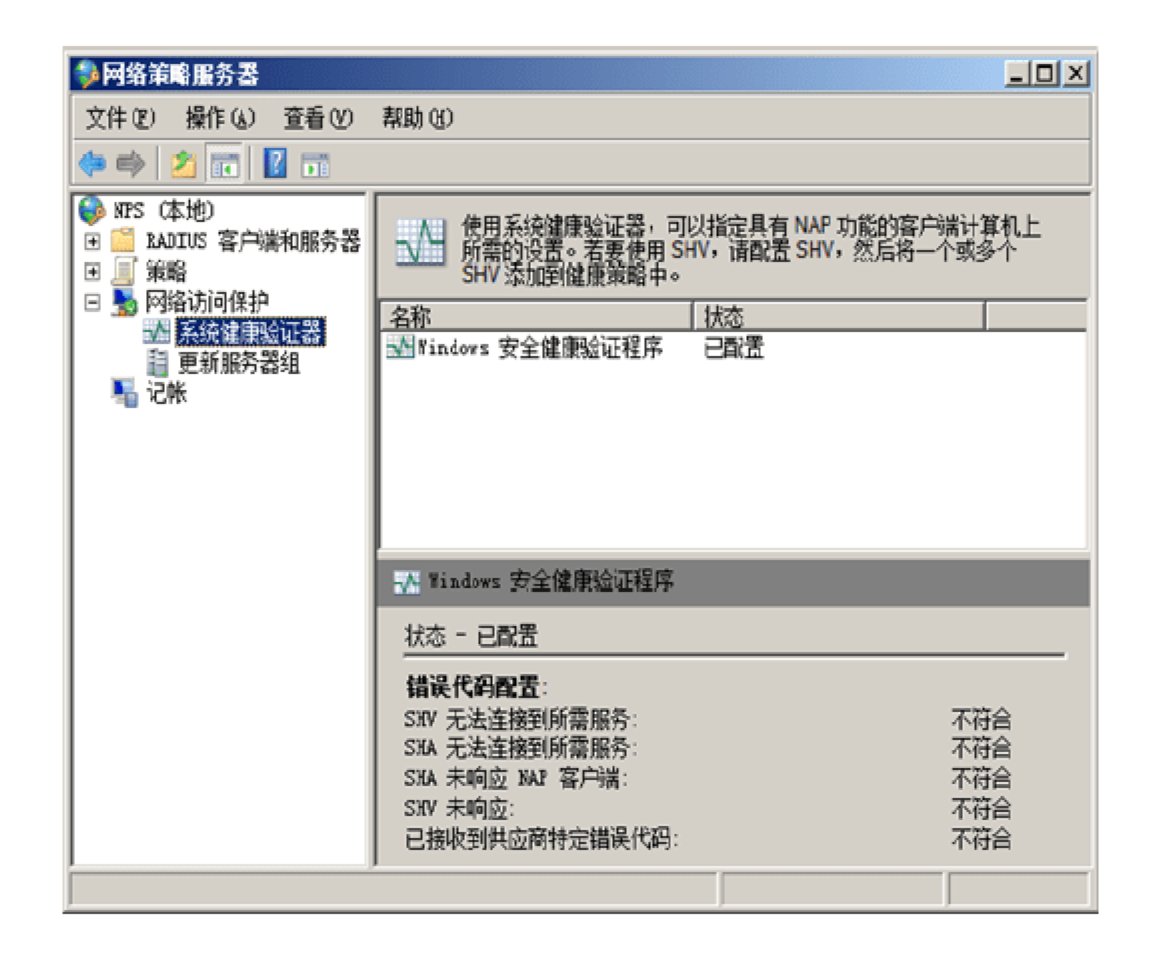
> **提示**　为了确保“配置 NAP”向导所配置的策略正确无误，还应再一一检查每条策略的执行顺序、条件、约束和设置等。

3. 配置系统健康验证器

在 NPS 服务器中，要根据客户端计算机的健康要求，配置系统健康验证器（SHV）来对客户端计算机进行验证。Windows 安全健康验证程序中包括防火墙、自动更新、防病毒程序、防间谍软件等审核对象。

01 在“网络策略服务器”窗口中，依次展开“网络访问保护”→“系统健康验证器”选项，默认已创建了一个系统健康验证器。选择“Windows 安全健康验证程序”，右击并选择快捷菜单中的“属性”选项，显示“Windows 系统健康验证程序 属性”对话框，可以根据系统健康要求配置每个 SHV，如图 16.71 所示。





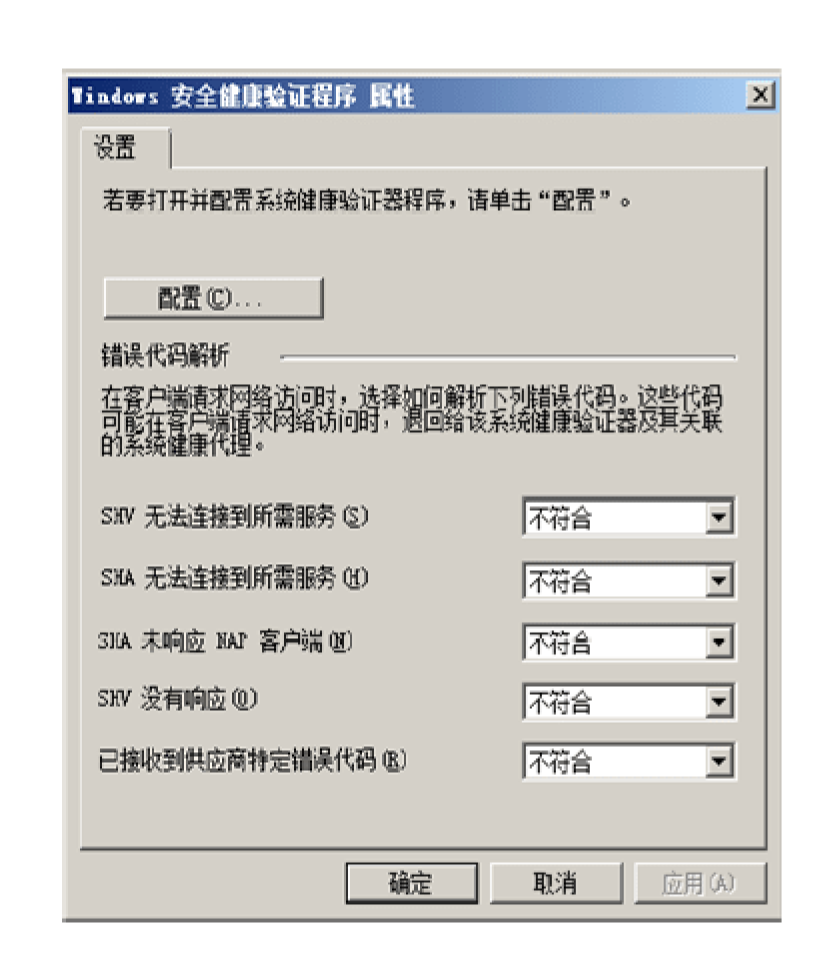


图 16.71　在“系统健康验证程序”窗口配置 SHV

02 单击“配置”按钮，显示如图 16.72 所示“Windows 安全健康验证程序”对话框。在“Windows Vista”选项卡中，可以设置对 Windows Vista 系统的安全健康验证程序策略。如果同时要验证客户端系统的安全更新程序，可选中“限制对未安装所有可用安全更新的客户端的访问权限”复选框，并设置客户端接收安全更新的方式。

03 在“Windows XP”选项卡中，用来配置 Windows XP SP3 的系统安全健康验证，如图 16.73 所示。

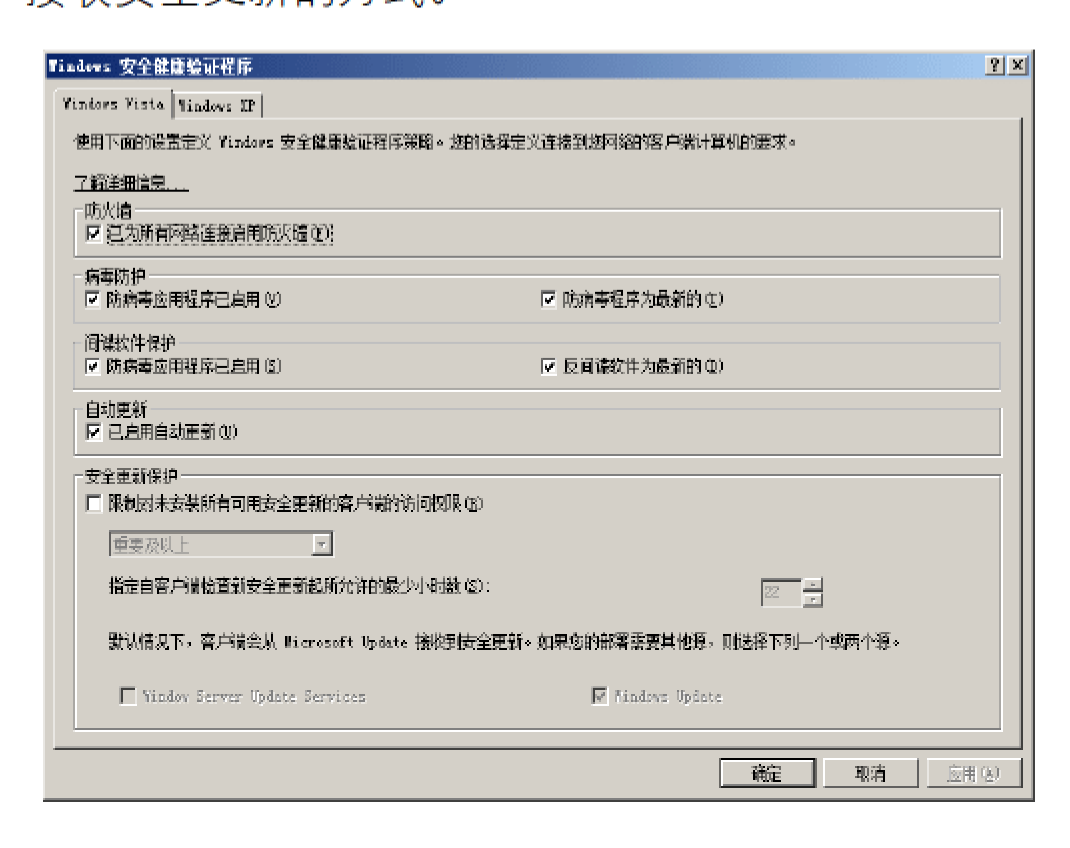


图 16.72　“Windows 安全健康验证程序”对话框

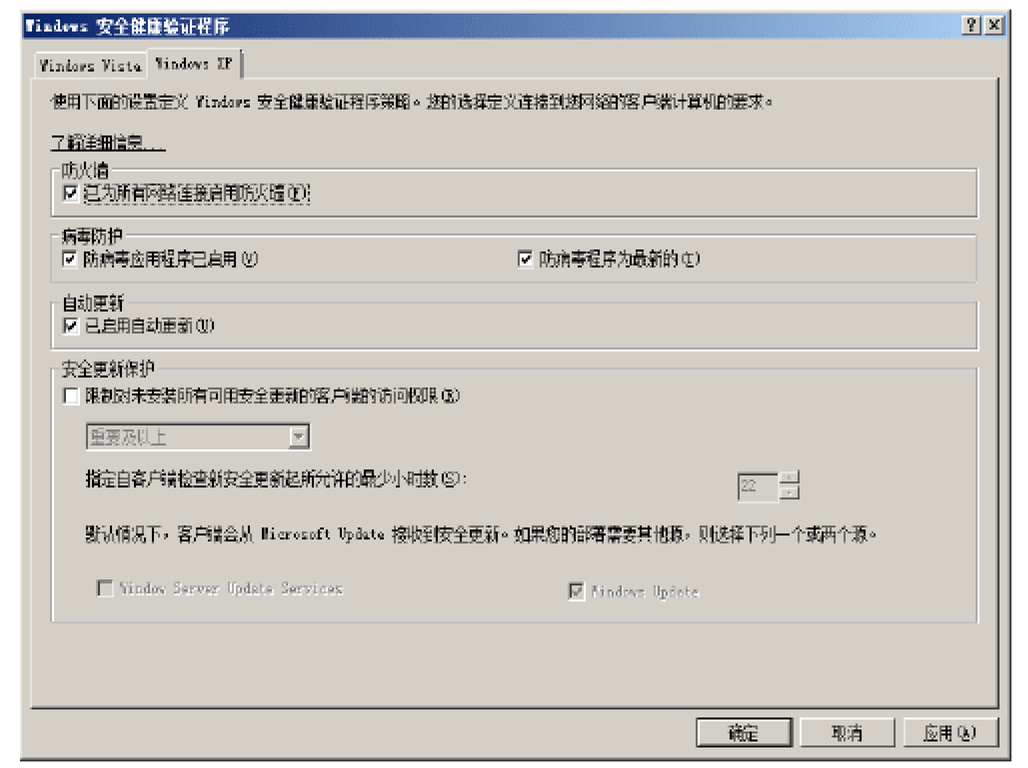


图 16.73　Windows XP 系统安全健康验证

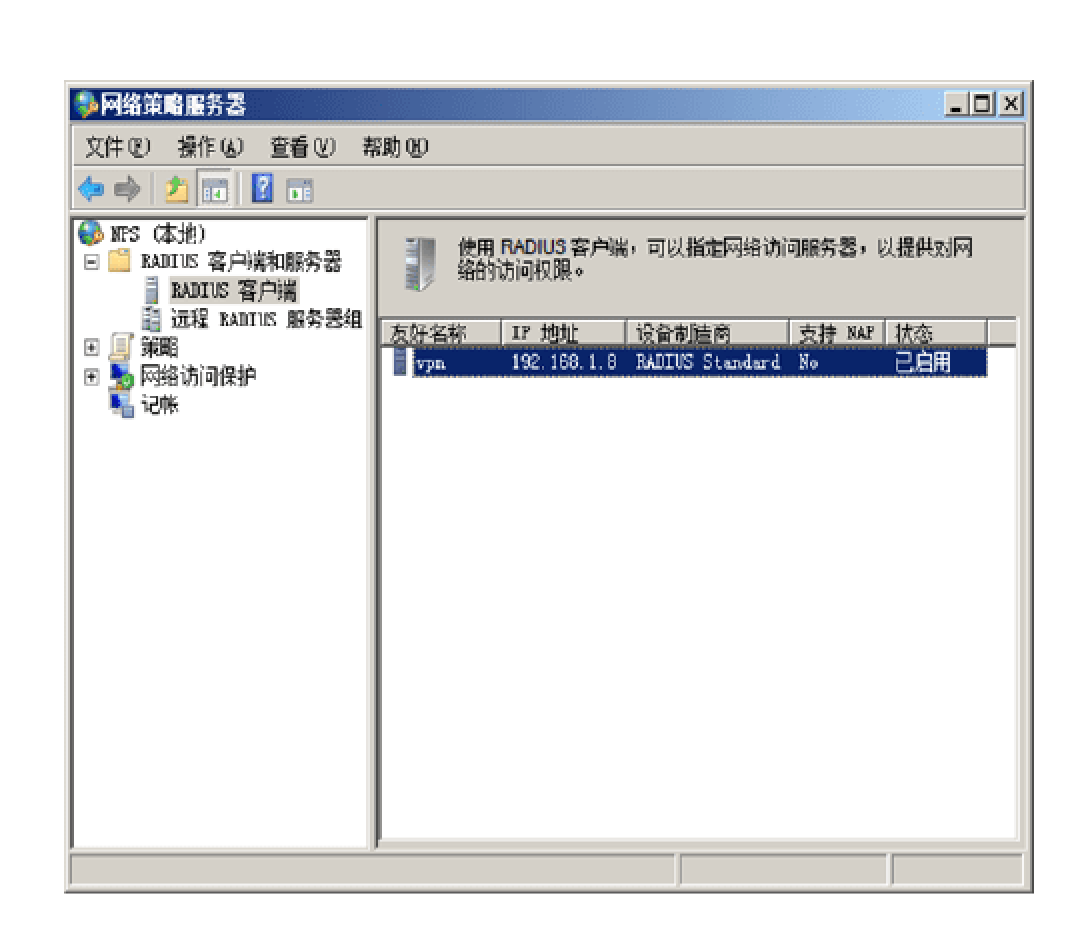
04 设置完成后单击“确定”按钮保存即可。

4. 为 RADIUS 客户端配置 NAP 支持

在安装 VPN 服务器时，设置了 RAIUS 服务器。因此在 NPS 服务器中也应启用 RADIUS 客户端，该客户端就是 VPN 服务器，使 VPN 服务器与 RADIUS 服务器能够连接。

在“网络策略服务器”窗口中，依次展开“RADIUS 客户端和服务器”→“RADIUS 客户端”，在右侧窗口列出了已配置的 RADIUS 客户端。右击名称为“VPN”的 RADIUS 客户端，选择快捷菜单中的“属性”选项，显示如图 16.74 所示“VPN 属性”对话框，选中“RADIUS

客户端支持 NAP”复选框。最后，单击“确定”按钮保存即可。



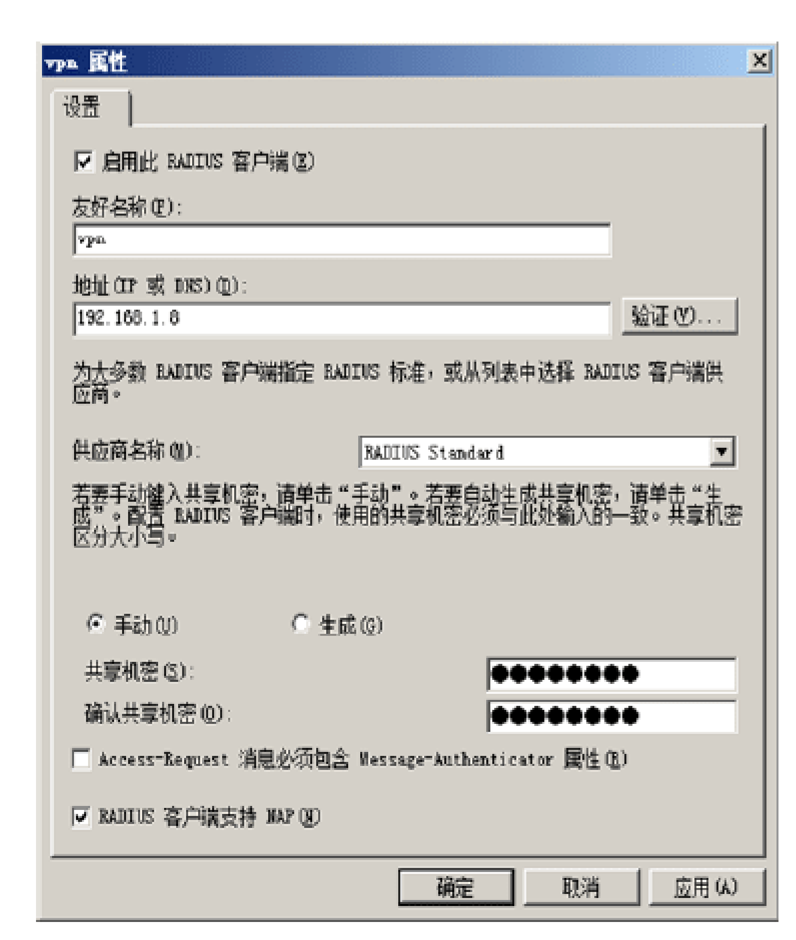


图 16.74　设置 RADIUS 客户端支持 NAP

16.6.3　配置 VPN 强制客户端

DHCP 强制客户端的配置过程与 IPSec 强制客户端类似，不同的是，在配置 NAP 客户端代理组件时，应启用“远程访问隔离强制客户端”选项，如图 16.75 所示。其他配置操作完全相同，此处不复赘述。



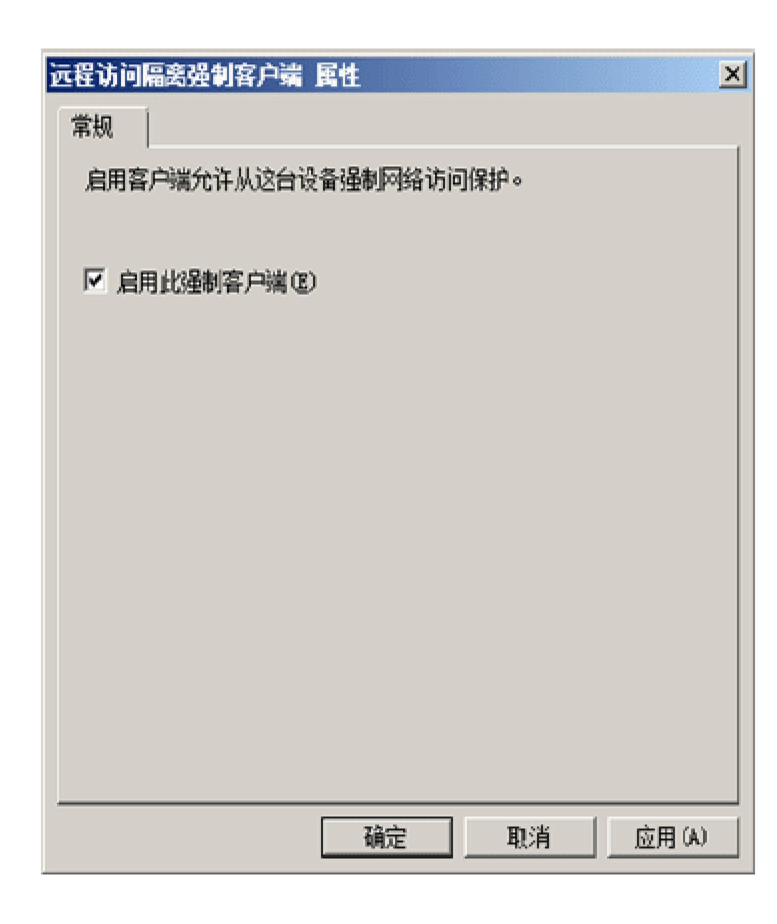


图 16.75　设置远程访问隔离强制客户端 属性

16.6.4　客户端访问受保护的 VPN 服务器

当配置了网络访问保护策略以后，在 VPN 客户端上使用原来的 VPN 连接就无法连接 VPN 服务器了，必须先在客户端计算机上配置证书信任和身份验证协议。当 VPN 客户端拨入 VPN 服务器并通过网络访问策略验证以后，方可正常访问内部网络，否则访问将会受到限制。



1. 设置证书信任

VPN 客户端必须从内部网络的证书服务器上下载证书并安装到“受信任的证书颁发机构”中，使其信任证书服务器，才可以连接 VPN 服务器。

01 以 Windows Vista 操作系统为例。打开 IE 浏览器，在地址栏中输入证书服务器的地址，格式为：http://证书服务器地址/certsrvn 回车，提示需要登录，如图 16.76 所示。

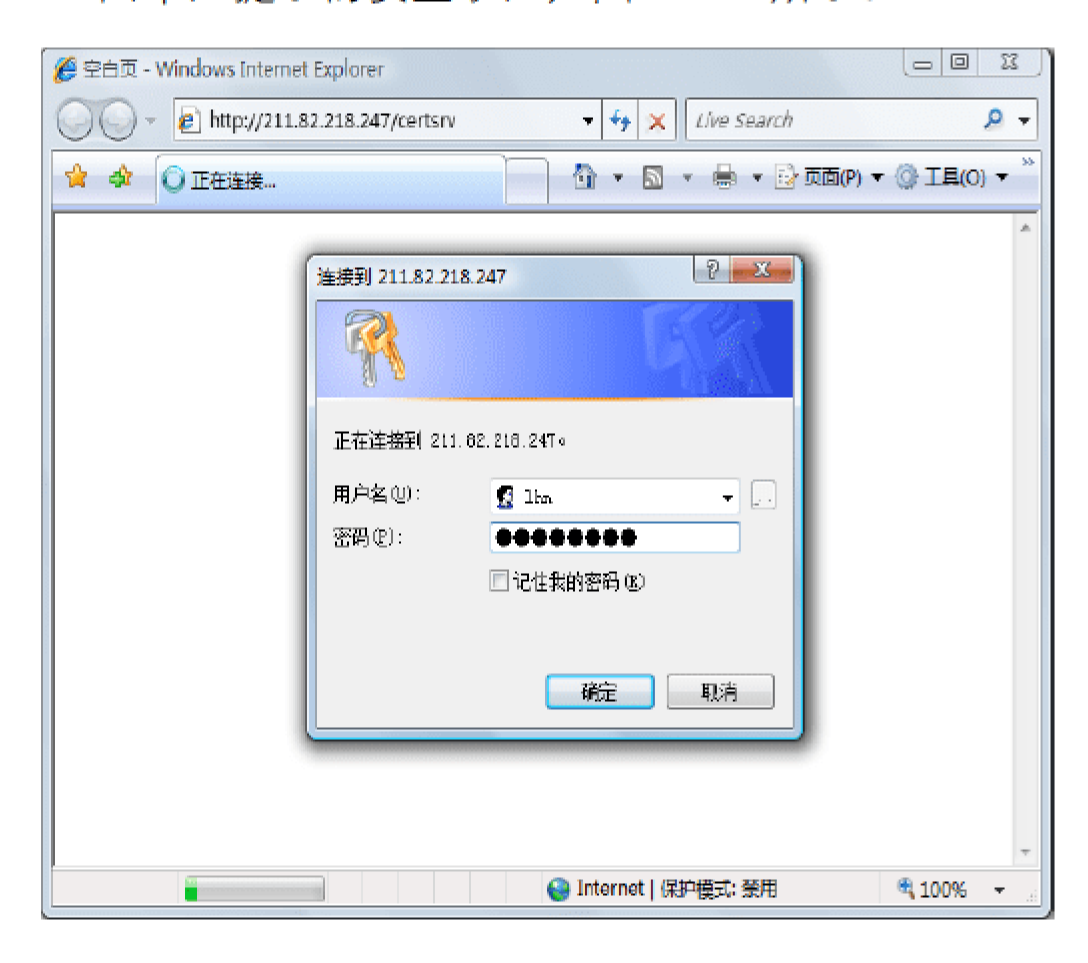


图 16.76　登录证书服务器

02 在“用户名”和“密码”文本框中键入域用户帐户名和密码，单击“确定”按钮，即可打开证书服务页面。单击“下载 CA 证书、证书链或 CRL”超级链接，显示“下载 CA 证书、证书链接或 CRL”窗口。单击“下载 CA 证书”超级链接，显示“文件下载-安全警告”对话框。单击“保存”按钮，将证书下载到本地计算机。如图 16.77 所示。

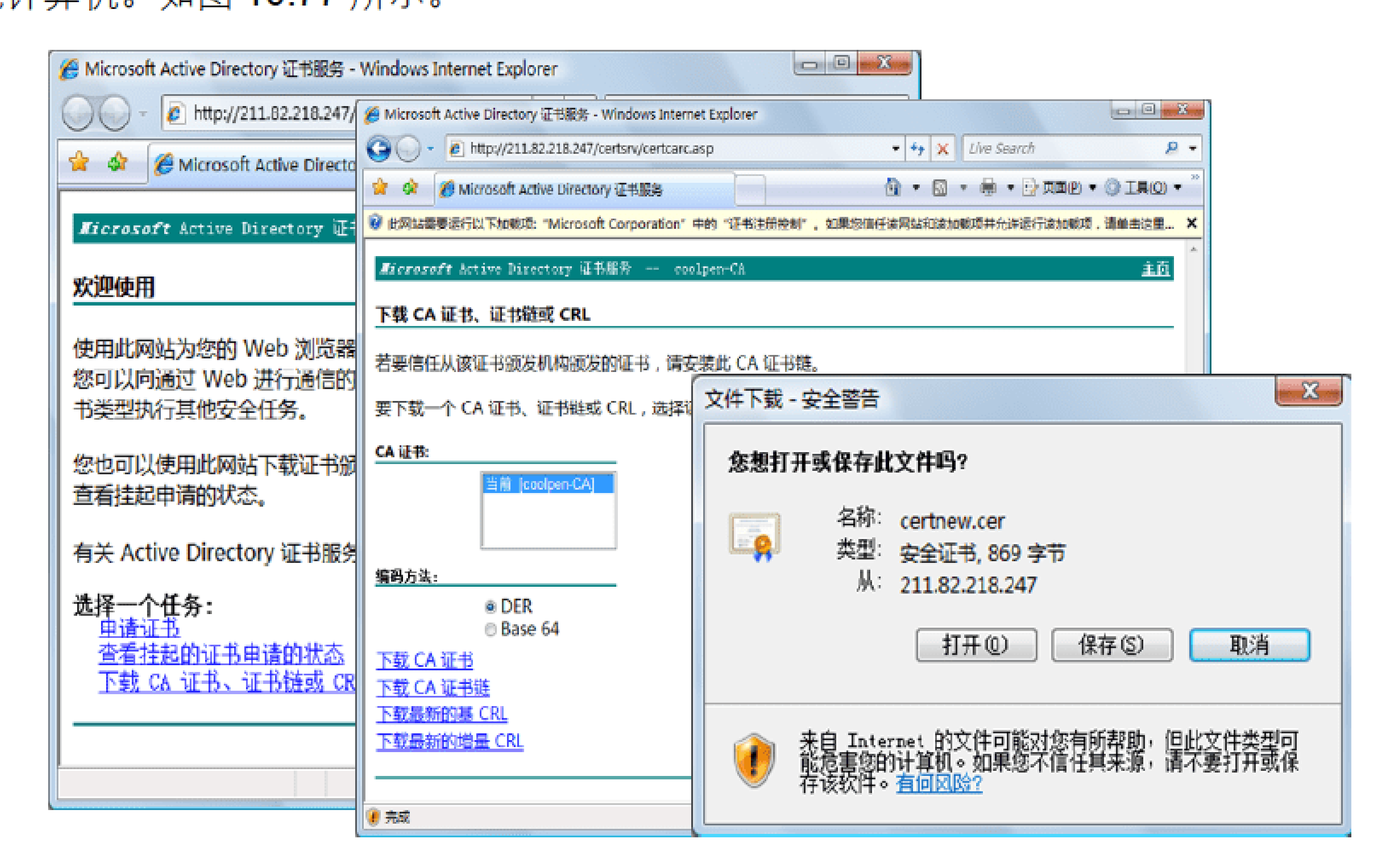
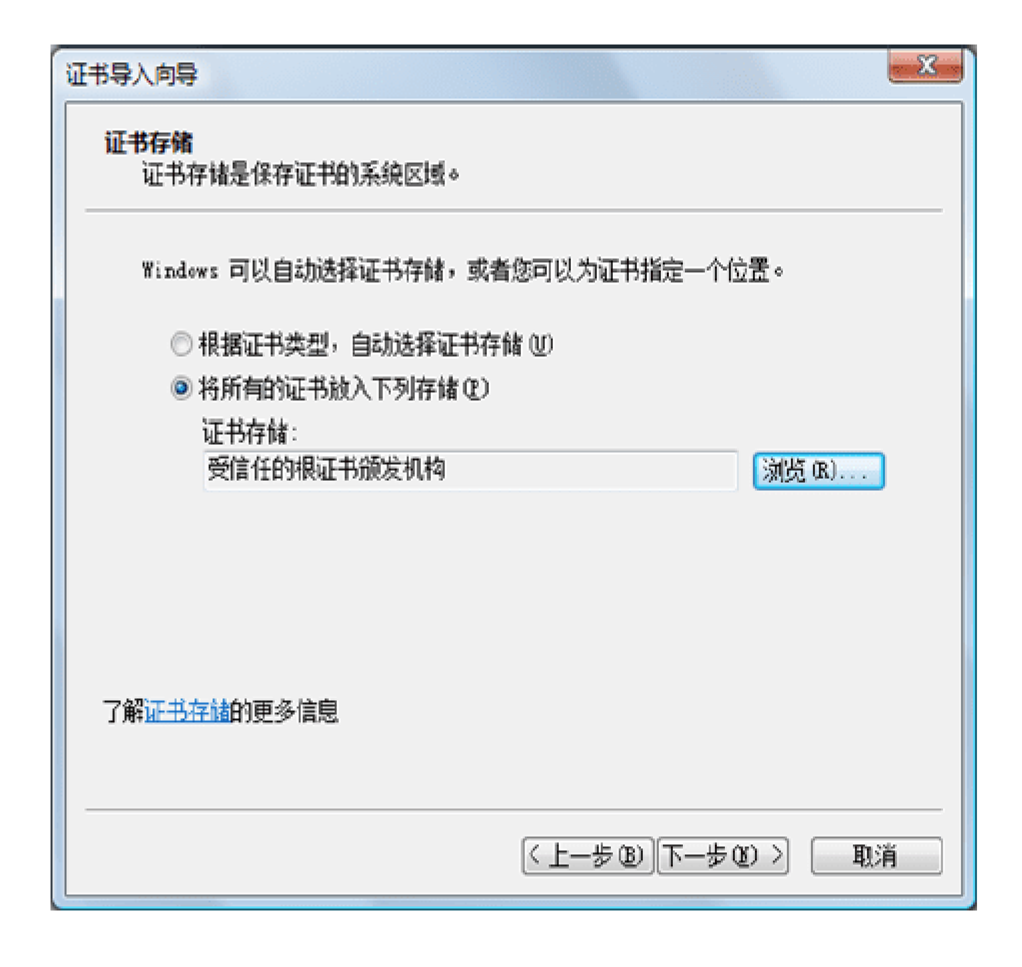


图 16.77　下载证书

03 右击所下载的证书并选择快捷菜单中的“安装证书”选项，启动“证书导入向导”。单击“下一步”按钮，显示“证书存储”对话框，选择“将所有的证书放入下列存储”单选按钮，并单击“浏览”按钮，选择“受信任的根证书颁发机构”。依次单击“下一步”按钮，完全使用默认设置即可，直至向导完成。如图 16.78 所示。



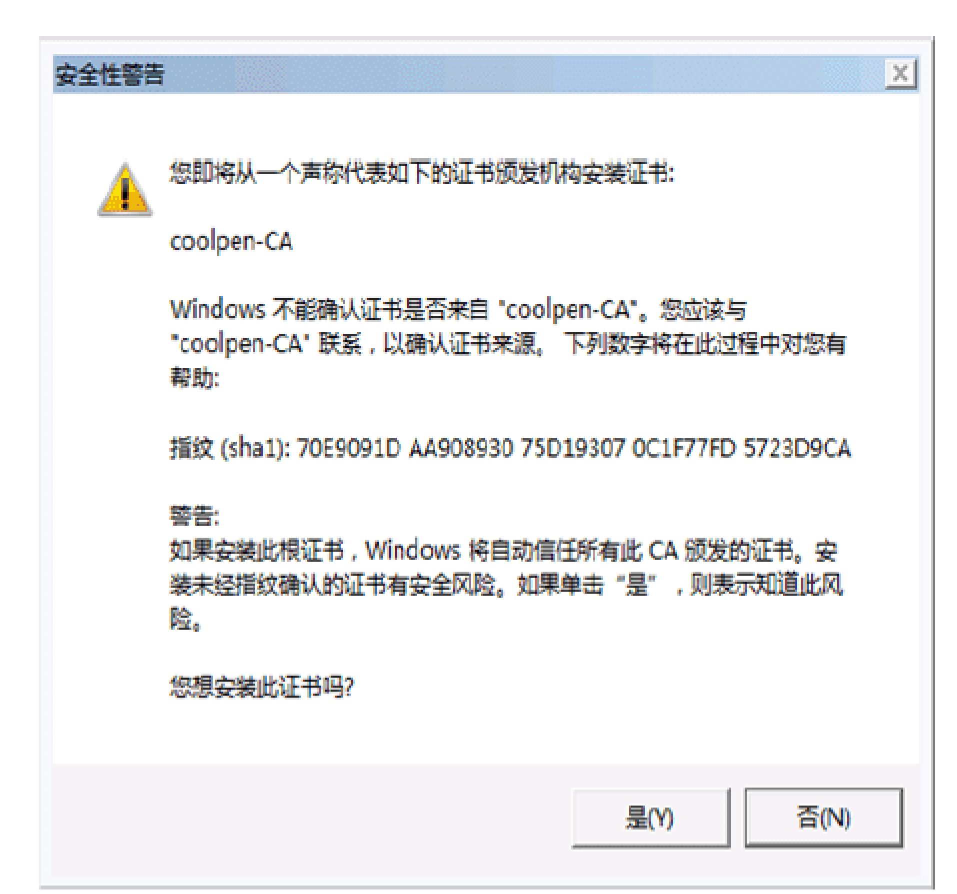


图 16.78　安装证书

2. 配置身份验证协议

01 在“网络和共享中心”窗口中，单击“管理网络连接”，打开“网络连接”窗口。选择已创建的 VPN 链接，右击并选择快捷菜单中的“属性”选项，显示“VPN 连接 属性”对话框。切换到“安全”选项卡，选择“高级（自定义设置）”单选按钮，如图 16.79 所示。

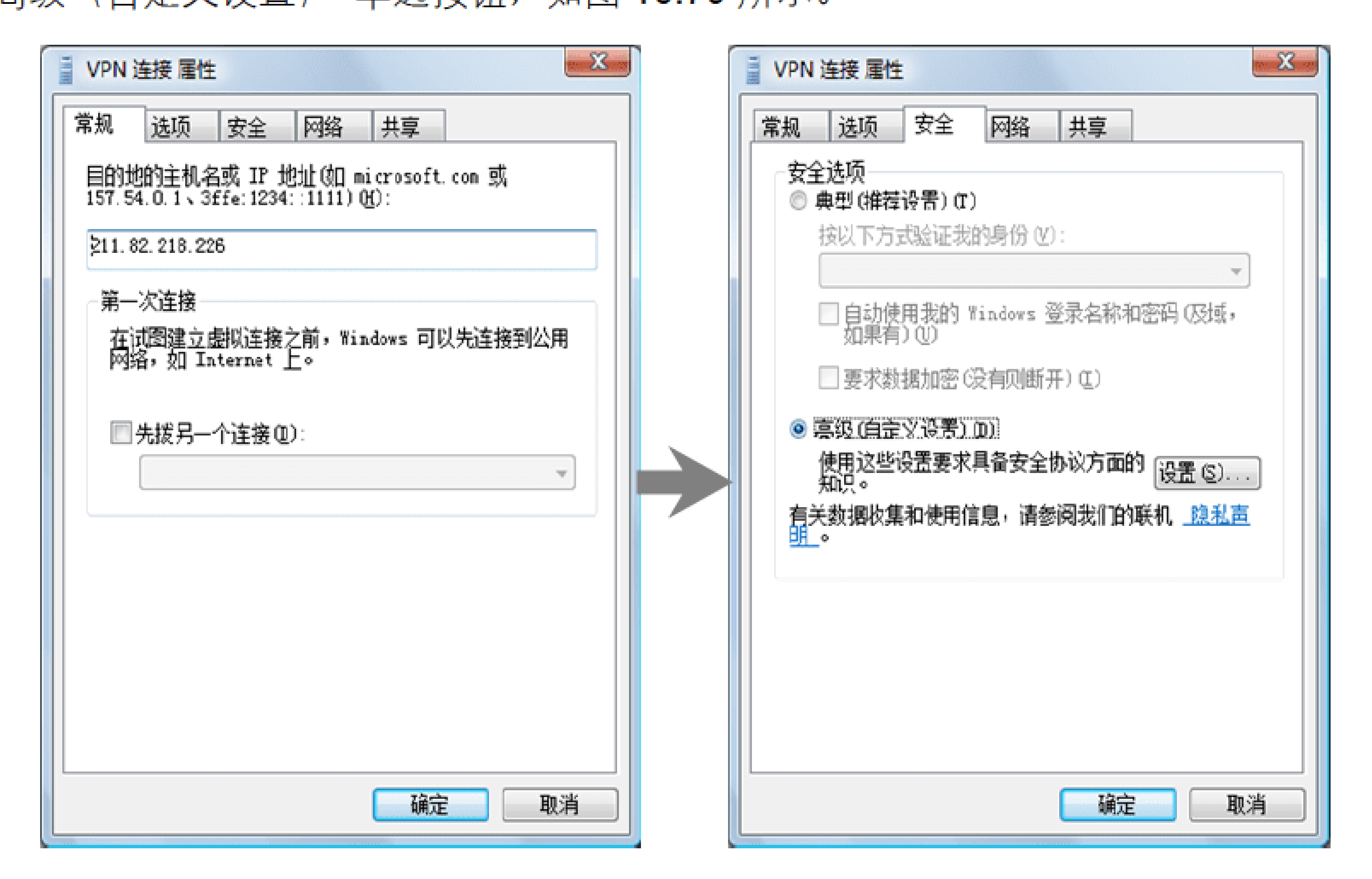


图 16.79　设置“安全”选项卡

02 单击“设置”按钮，显示如图 16.80 所示“高级安全设置”对话框，在“数据加密”下拉列表中选择“需要加密（如果服务器拒绝将断开连接）”选项。选择“使用可扩展的身份验证协议（EAP）”单选按钮，并在下拉列表中选择“受保护的 EAP (PEAP) (启用加密)”选项。

03 单击“属性”按钮，显示如图 16.81 所示“受保护的 EAP 属性”对话框，确认选中“验证服务器证书”文本框，并取消“连接到这些服务器”复选框。在“受信任的根证书颁发机构”列表框中，可以看到已经安装的证书颁发机构。在“选择身份验证方法”下拉列表中，选择“安全密码”选项，并选中“启用隔离检查”复选框。



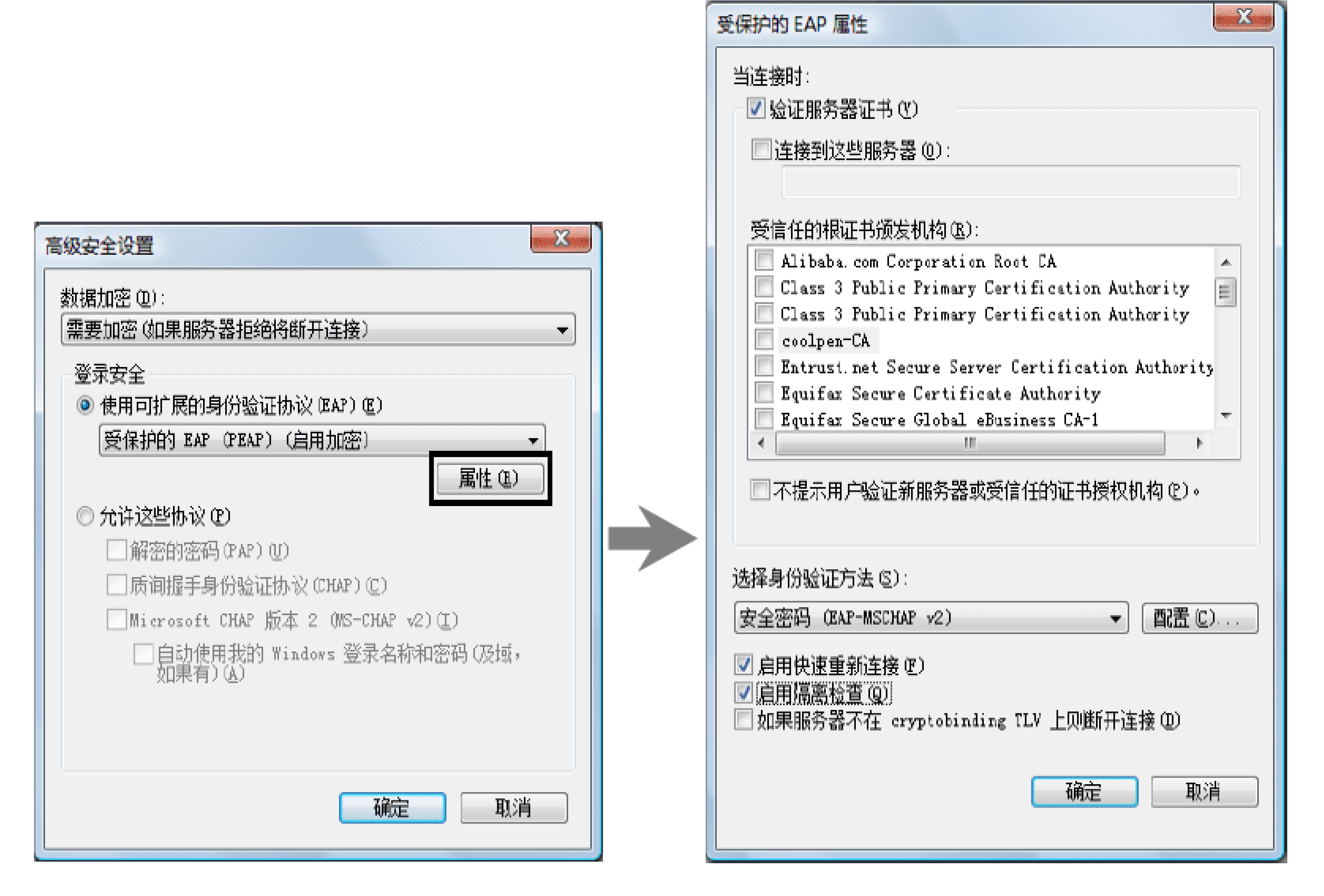


图 16.80 “高级安全设置”对话框　　图 16.81 “受保护的 EAP 属性”对话框

04 依次单击“确定”按钮保存即可。

3. 使用 VPN 连接内部网络

01 在“网络连接”窗口中，双击已创建的 VPN 连接，显示“连接 VPN 连接”对话框。单击“连接”按钮，显示如图 16.82 所示“输入凭据”对话框，可以设置要拨入 VPN 服务器的帐户和密码。



图 16.82 打开“输入凭据”对话框

02 单击“确定”按钮，开始连接 VPN 服务器，并验证用户名和密码。验证通过以后，显示如图 16.83 所示“验证服务器证书”对话框，要求确认服务器证书是否正确。

03 单击“确定”按钮，连接 VPN 网络。如果客户端计算机的配置不符合网络访问保护策略的要求，就会在桌面右下角的托盘区域中显示如图 16.84 所示“此计算机不符合该网络的要求”的提示。

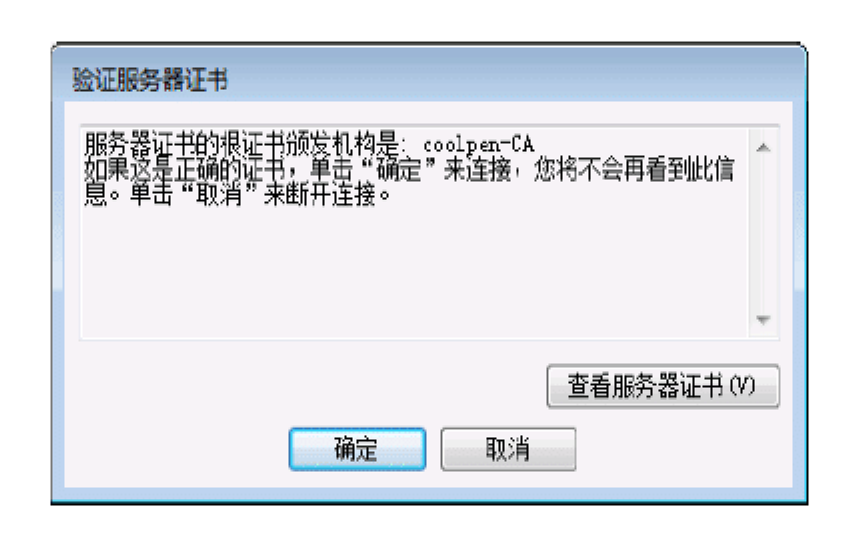


图 16.83 "验证服务器证书"对话框

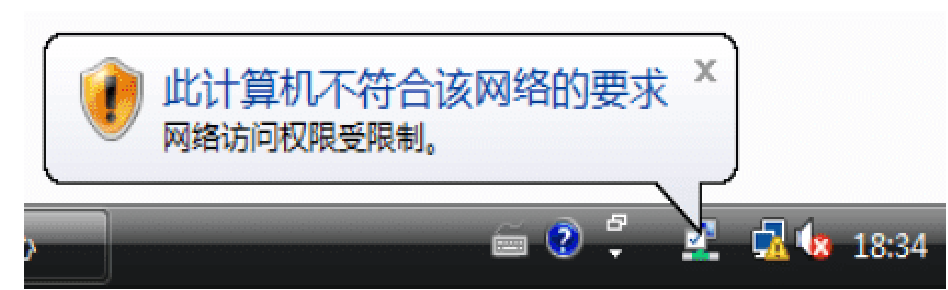


图 16.84 此计算机不符合该网络的要求

04 此时，VPN 强制会根据网络访问保护策略，自动修正客户端计算机的设置，如 Windows 防火墙、自动更新等，如图 16.85 所示。

05 当客户端计算机的配置被启用以后，符合网络要求，会显示如图 16.86 所示"此计算机符合该网络的要求"的提示，此时，计算机即可拥有访问 VPN 网络的完全权限了。

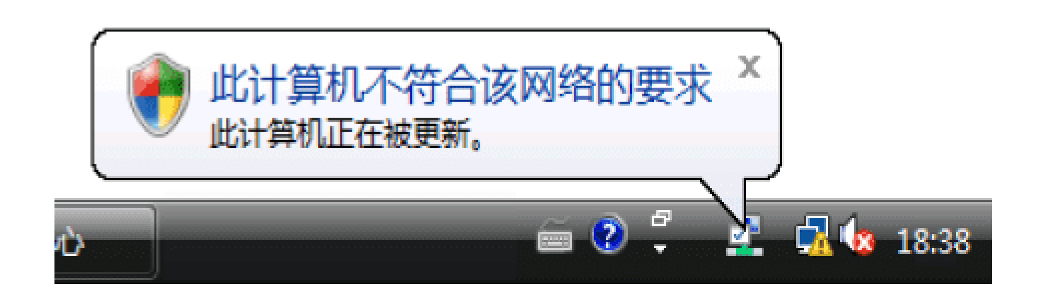


图 16.85 计算机正在被更新

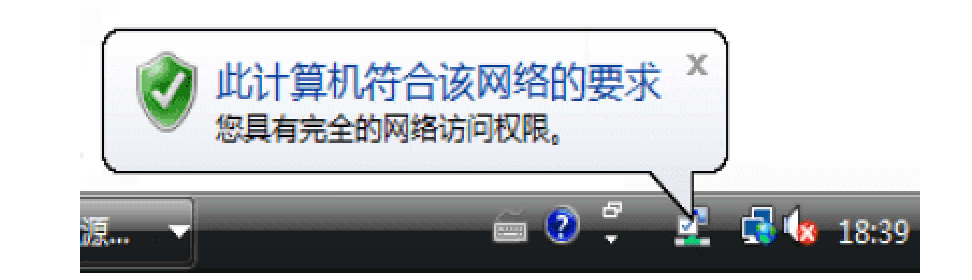


图 16.86 此计算机符合该网络的要求

不过，如果经过 VPN 强制以后，仍然不符合网络访问保护策略，那么该计算机的访问仍然受限。例如，VPN 强制可以启用系统的 Windows 防火墙和自动更新，但不能强制安装杀毒软件，因此，单击提示信息，显示如图 16.87 所示"网络访问保护"对话框，提示没有检测到防病毒程序，该计算机的网络访问权限也受到限制。

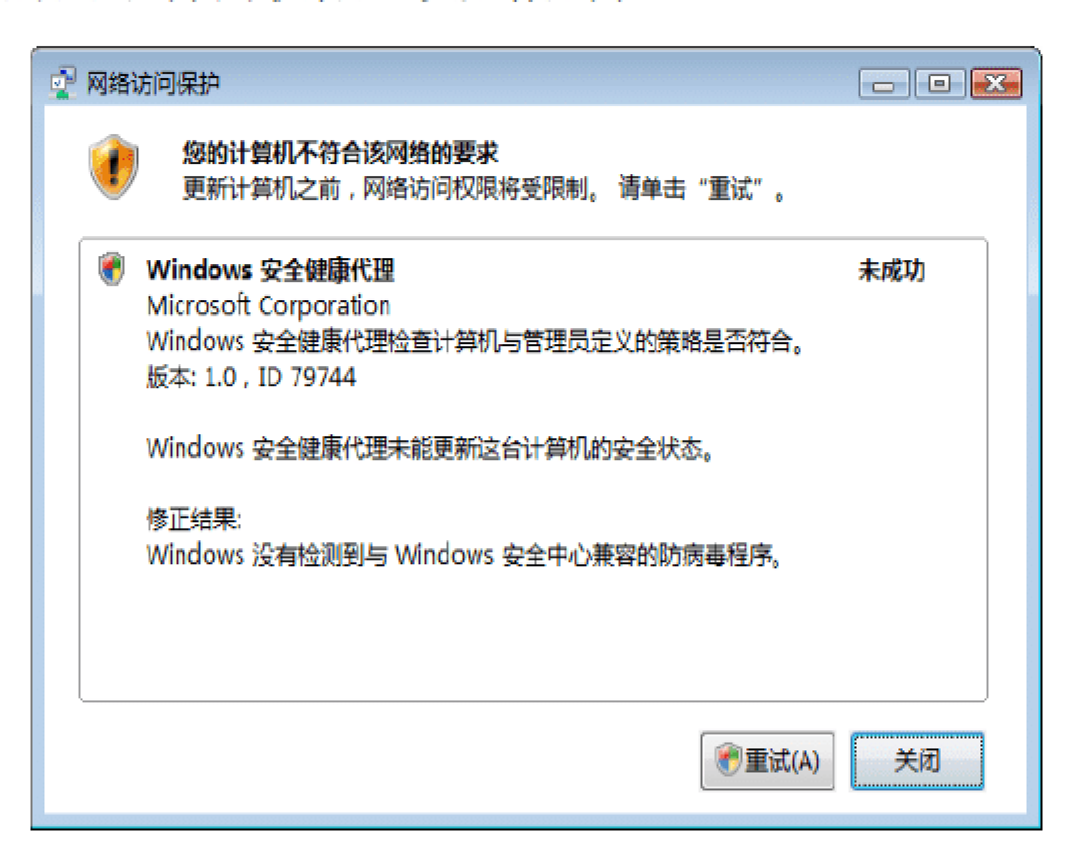


图 16.87 "网络访问保护"对话框

小　　结

NAP 是 Windows Server 2008 系统新增功能之一，通过对客户端进行健康评估，只有达到网络健康标准客户端，才允许接入内部网络，否则将被隔离，直至恢复健康状态。本章主要介绍了 NAP 在局域网中的几种常见应用，包括 IPSec 强制、DHCP 强制和 VPN 强制。IPSec 策



略是基于 IP 数据包的筛选机制，IPSec 强制系统主要用于确保网络通信双方系统的健康程度，从而确保网络访问安全。DHCP 强制主要用于配合其他强制系统使用，用于为隔离网络和健康网络分配不同类型的 IP 地址。VPN 强制主要用于验证远程访问用户计算机系统的健康程度，避免其携带危险因素进入局域网。NAP 只能对用户计算机健康状态进行评估，并不能代替杀毒软件、防火墙等安全防护设备，用户应用时应十分注意。

习　　题

1. NAP 简介。
2. NAP 有哪些功能？
3. NAP 有哪些组件？
4. NAP 的不足之处有哪些？

实验：配置 802.1X 强制

实验目的

802.1X 强制也是 NAP 的一项重要应用，可以用于交换机、AP 等接入设备的身份验证。

实验内容

使用 802.1X 身份验证的无线 AP 或启动 802.1X 的交换机，来限制不符合的 NAP 客户端的访问。

实验步骤

1. 配置活动目录。
2. 配置基于 PEAP 的身份验证方式。
3. 配置 802.1X 访问点。
4. 配置受限网络中的更新服务器。
5. 配置 NAP 健康策略服务器。
6. 配置 NAP 客户端。
7. 为报告模式的 802.1X 强制配置查点。
8. 测试受限访问。
9. 为不符合的 NAP 客户端的延期强制配置网络策略。
10. 为强制模式配置网络策略。



SQL Server 数据库安全

现在以 ASP、PHP、JSP 为主的动态网站都涉及到数据库的应用，许多管理员往往只重视操作系统本身的漏洞而忽略了数据库和一些脚本的安全设置，给网站埋下了安全隐患。Windows Server 2008 是一个“缺省安全”的产品，默认情况下整个服务器被锁定，网络管理员须亲自启动每个需要使用的服务。在 SQL Server 2005 中，默认情况下，整个数据库服务器也是被锁定的，需管理员手工激活才能使用。

本章导读

- 数据库安全设置
- MBSA 数据库扫描
- 数据备份与安全
- 系统补丁



17.1　数据库安全设置

SQL Server 数据库中存储企业和网站的重要数据，因此是很多入侵者攻击的主要对象，通过对数据库的合理设置，从而提高数据库的安全性，降低被入侵的风险性。

17.1.1　文件夹访问权限

NTFS 文件系统的磁盘具有严格的用户访问权限，为了保护数据库的安全。可以将 SQL Server 数据库安装在 NTFS 分区上，再设置适当的权限，降低入侵者通过文件操作权限来破坏数据库的可行性。

1. 文件夹安全设置

数据库文件默认存储在 SQL Server 安装目录下的子文件夹中，管理员可以通过设置有许可的用户才能访问这个文件夹来保护数据库的安全。

01 右击“Microsoft SQL Server”文件夹，在快捷菜单中选择“属性”选项，打开如图 17.1 所示的“Microsoft SQL Server 属性”窗口。



图 17.1　“Microsoft SQL Server 属性”窗口

02 切换至“安全”选项卡，删除除指定许可的用户或组以外的其他用户和组，单击“确定”按钮保存设置即可。

> 提示　建议取消除 Administrator 组具备的“完全控制”权限以外，其他用户或组不分配“完全控制权限”。



17.1 数据库安全设置

SQL Server 数据库中存储企业和网站的重要数据，因此是很多入侵者攻击的主要对象，通过对数据库的合理设置，从而提高数据库的安全性，降低被入侵的风险性。

17.1.1 文件夹访问权限

NTFS 文件系统的磁盘具有严格的用户访问权限，为了保护数据库的安全。可以将 SQL Server 数据库安装在 NTFS 分区上，再设置适当的权限，降低入侵者通过文件操作权限来破坏数据库的可行性。

1. 文件夹安全设置

数据库文件默认存储在 SQL Server 安装目录下的子文件夹中，管理员可以通过设置有许可的用户才能访问这个文件夹来保护数据库的安全。

01 右击“Microsoft SQL Server”文件夹，在快捷菜单中选择“属性”选项，打开如图 17.1 所示的“Microsoft SQL Server 属性”窗口。



图 17.1 “Microsoft SQL Server 属性”窗口

02 切换至“安全”选项卡，删除除指定许可的用户或组以外的其他用户和组，单击“确定”按钮保存设置即可。

提示 建议取消除 Administrator 组具备的“完全控制”权限以外，其他用户或组不分配“完全控制权限”。



17.1　数据库安全设置

SQL Server 数据库中存储企业和网站的重要数据，因此是很多入侵者攻击的主要对象，通过对数据库的合理设置，从而提高数据库的安全性，降低被入侵的风险性。

17.1.1　文件夹访问权限

NTFS 文件系统的磁盘具有严格的用户访问权限，为了保护数据库的安全。可以将 SQL Server 数据库安装在 NTFS 分区上，再设置适当的权限，降低入侵者通过文件操作权限来破坏数据库的可行性。

1. 文件夹安全设置

数据库文件默认存储在 SQL Server 安装目录下的子文件夹中，管理员可以通过设置有许可的用户才能访问这个文件夹来保护数据库的安全。

01　右击“Microsoft SQL Server”文件夹，在快捷菜单中选择“属性”选项，打开如图 17.1 所示的“Microsoft SQL Server 属性”窗口。



图 17.1　“Microsoft SQL Server 属性”窗口

02　切换至“安全”选项卡，删除除指定许可的用户或组以外的其他用户和组，单击“确定”按钮保存设置即可。

提示　建议取消除 Administrator 组具备的“完全控制”权限以外，其他用户或组不分配“完全控制权限”。



17.1　数据库安全设置

SQL Server 数据库中存储企业和网站的重要数据，因此是很多入侵者攻击的主要对象，通过对数据库的合理设置，从而提高数据库的安全性，降低被入侵的风险性。

17.1.1　文件夹访问权限

NTFS 文件系统的磁盘具有严格的用户访问权限，为了保护数据库的安全。可以将 SQL Server 数据库安装在 NTFS 分区上，再设置适当的权限，降低入侵者通过文件操作权限来破坏数据库的可行性。

1. 文件夹安全设置

数据库文件默认存储在 SQL Server 安装目录下的子文件夹中，管理员可以通过设置有许可的用户才能访问这个文件夹来保护数据库的安全。

01 右击“Microsoft SQL Server”文件夹，在快捷菜单中选择“属性”选项，打开如图 17.1 所示的“Microsoft SQL Server 属性”窗口。



图 17.1　“Microsoft SQL Server 属性”窗口

02 切换至“安全”选项卡，删除除指定许可的用户或组以外的其他用户和组，单击“确定”按钮保存设置即可。

> 提示　建议取消除 Administrator 组具备的“完全控制”权限以外，其他用户或组不分配“完全控制权限”。



17.1　数据库安全设置

SQL Server 数据库中存储企业和网站的重要数据，因此是很多入侵者攻击的主要对象，通过对数据库的合理设置，从而提高数据库的安全性，降低被入侵的风险性。

17.1.1　文件夹访问权限

NTFS 文件系统的磁盘具有严格的用户访问权限，为了保护数据库的安全。可以将 SQL Server 数据库安装在 NTFS 分区上，再设置适当的权限，降低入侵者通过文件操作权限来破坏数据库的可行性。

1. 文件夹安全设置

数据库文件默认存储在 SQL Server 安装目录下的子文件夹中，管理员可以通过设置有许可的用户才能访问这个文件夹来保护数据库的安全。

01 右击“Microsoft SQL Server”文件夹，在快捷菜单中选择“属性”选项，打开如图 17.1 所示的“Microsoft SQL Server 属性”窗口。



图 17.1　“Microsoft SQL Server 属性”窗口

02 切换至“安全”选项卡，删除除指定许可的用户或组以外的其他用户和组，单击“确定”按钮保存设置即可。

> 提示　建议取消除 Administrator 组具备的“完全控制”权限以外，其他用户或组不分配“完全控制权限”。



17.1　数据库安全设置

SQL Server 数据库中存储企业和网站的重要数据，因此是很多入侵者攻击的主要对象，通过对数据库的合理设置，从而提高数据库的安全性，降低被入侵的风险性。

17.1.1　文件夹访问权限

NTFS 文件系统的磁盘具有严格的用户访问权限，为了保护数据库的安全。可以将 SQL Server 数据库安装在 NTFS 分区上，再设置适当的权限，降低入侵者通过文件操作权限来破坏数据库的可行性。

1. 文件夹安全设置

数据库文件默认存储在 SQL Server 安装目录下的子文件夹中，管理员可以通过设置有许可的用户才能访问这个文件夹来保护数据库的安全。

01 右击“Microsoft SQL Server”文件夹，在快捷菜单中选择“属性”选项，打开如图 17.1 所示的“Microsoft SQL Server 属性”窗口。



图 17.1　“Microsoft SQL Server 属性”窗口

02 切换至“安全”选项卡，删除除指定许可的用户或组以外的其他用户和组，单击“确定”按钮保存设置即可。

> 提示　建议取消除 Administrator 组具备的“完全控制”权限以外，其他用户或组不分配“完全控制权限”。



17.1　数据库安全设置

SQL Server 数据库中存储企业和网站的重要数据，因此是很多入侵者攻击的主要对象，通过对数据库的合理设置，从而提高数据库的安全性，降低被入侵的风险性。

17.1.1　文件夹访问权限

NTFS 文件系统的磁盘具有严格的用户访问权限，为了保护数据库的安全。可以将 SQL Server 数据库安装在 NTFS 分区上，再设置适当的权限，降低入侵者通过文件操作权限来破坏数据库的可行性。

1. 文件夹安全设置

数据库文件默认存储在 SQL Server 安装目录下的子文件夹中，管理员可以通过设置有许可的用户才能访问这个文件夹来保护数据库的安全。

01 右击“Microsoft SQL Server”文件夹，在快捷菜单中选择“属性”选项，打开如图 17.1 所示的“Microsoft SQL Server 属性”窗口。



图 17.1　“Microsoft SQL Server 属性”窗口

02 切换至“安全”选项卡，删除除指定许可的用户或组以外的其他用户和组，单击“确定”按钮保存设置即可。

> 提示　建议取消除 Administrator 组具备的“完全控制”权限以外，其他用户或组不分配“完全控制权限”。



17.1　数据库安全设置

SQL Server 数据库中存储企业和网站的重要数据，因此是很多入侵者攻击的主要对象，通过对数据库的合理设置，从而提高数据库的安全性，降低被入侵的风险性。

17.1.1　文件夹访问权限

NTFS 文件系统的磁盘具有严格的用户访问权限，为了保护数据库的安全。可以将 SQL Server 数据库安装在 NTFS 分区上，再设置适当的权限，降低入侵者通过文件操作权限来破坏数据库的可行性。

1. 文件夹安全设置

数据库文件默认存储在 SQL Server 安装目录下的子文件夹中，管理员可以通过设置有许可的用户才能访问这个文件夹来保护数据库的安全。

01 右击“Microsoft SQL Server”文件夹，在快捷菜单中选择“属性”选项，打开如图 17.1 所示的“Microsoft SQL Server 属性”窗口。



图 17.1　“Microsoft SQL Server 属性”窗口

02 切换至“安全”选项卡，删除除指定许可的用户或组以外的其他用户和组，单击“确定”按钮保存设置即可。

提示　建议取消除 Administrator 组具备的“完全控制”权限以外，其他用户或组不分配“完全控制权限”。



17.1　数据库安全设置

SQL Server 数据库中存储企业和网站的重要数据，因此是很多入侵者攻击的主要对象，通过对数据库的合理设置，从而提高数据库的安全性，降低被入侵的风险性。

17.1.1　文件夹访问权限

NTFS 文件系统的磁盘具有严格的用户访问权限，为了保护数据库的安全。可以将 SQL Server 数据库安装在 NTFS 分区上，再设置适当的权限，降低入侵者通过文件操作权限来破坏数据库的可行性。

1. 文件夹安全设置

数据库文件默认存储在 SQL Server 安装目录下的子文件夹中，管理员可以通过设置有许可的用户才能访问这个文件夹来保护数据库的安全。

01 右击“Microsoft SQL Server”文件夹，在快捷菜单中选择“属性”选项，打开如图 17.1 所示的“Microsoft SQL Server 属性”窗口。



图 17.1　“Microsoft SQL Server 属性”窗口

02 切换至“安全”选项卡，删除除指定许可的用户或组以外的其他用户和组，单击“确定”按钮保存设置即可。

> 提示　建议取消除 Administrator 组具备的“完全控制”权限以外，其他用户或组不分配“完全控制权限”。

2. 文件夹共享权限

如果确实需要共享数据库文件，应对共享文件夹进行相应的设置。

01 右击“Microsoft SQL Server”文件夹，在快捷菜单中选择“属性”选项，打开“Microsoft SQL Server 属性”对话框。切换至“共享”选项卡，单击“高级共享”按钮，显示“高级共享”对话框。

02 选中“共享此文件夹”复选框，在“将同时共享的用户数量限制为”文本框中输入同时共享的用户限制，单击“权限”按钮，显示如图 17.2 所示“Microsoft SQL Server 的权限”对话框。

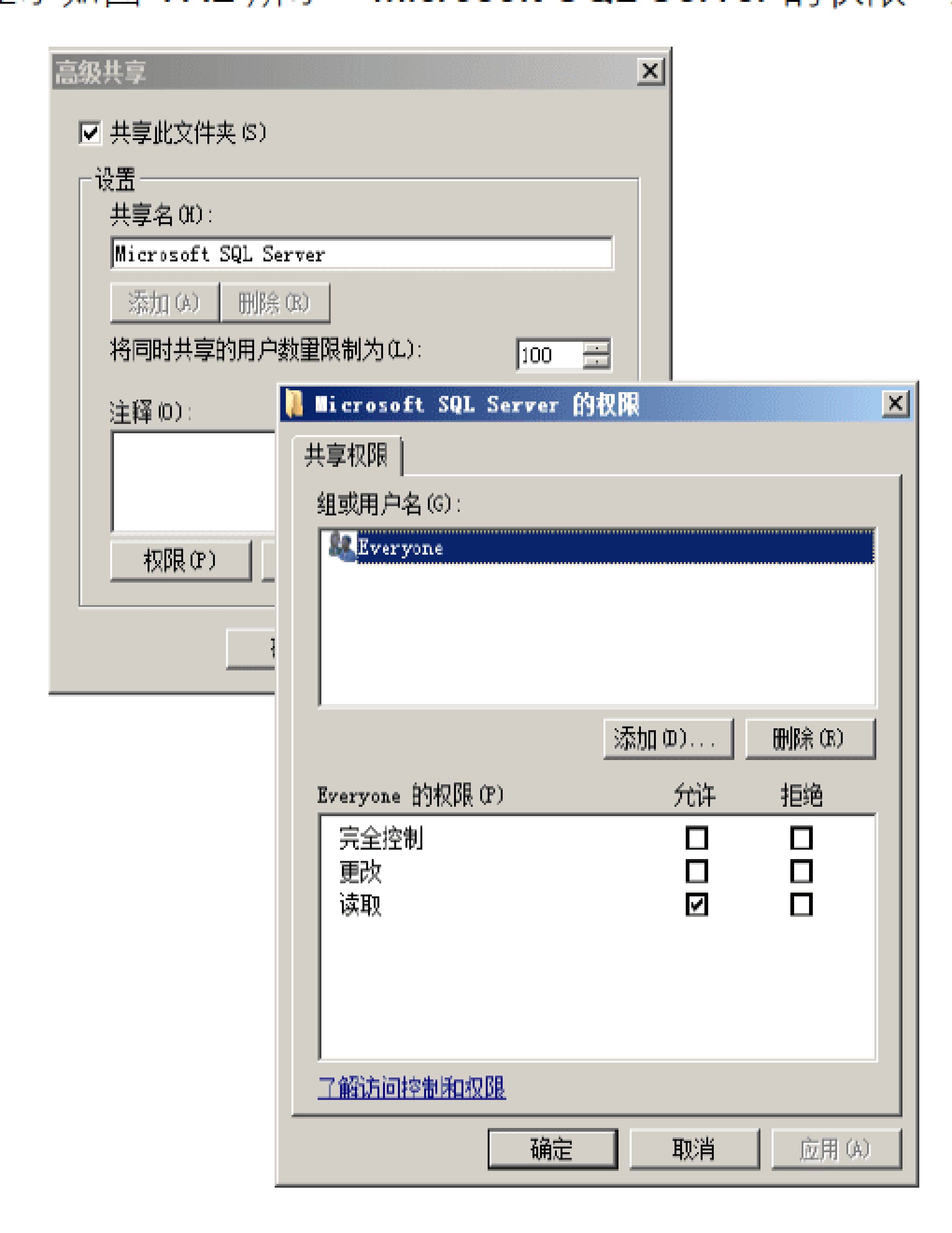


图 17.2　设置 Microsoft SQL Server 的共享权限

03 根据实际需要添加、删除组和用户名并设置相关权限。依次单击“确定”按钮，保存设置即可。

提示

除非情况特殊，否则不建议共享此文件夹。

17.1.2　数据库访问权限

Microsoft SQL Server 2005 可以定义登录用户的数据库访问权限和数据表的访问权限，下面将分别介绍对数据库和数据表访问权限设置的方法。

1. 数据库访问权限设置

通常情况下，只有授权的用户才能访问数据库，如果用户对数据库访问权限都没有，将不能访问数据库中数据表中的任何数据。



01 依次选择“开始”→“所有程序”→“Microsoft SQL Server 2005”→“Microsoft SQL Server Management Studio”，打开“Microsoft SQL Server Management Studio”窗口。依次选择“WIN-HKSLEYF2MMT”→“安全性”→“登录名”，在右侧窗口中右击需要设置访问权限的用户帐户（以 zhangsan 为例），在快捷菜单中选择“属性”选项，打开“登录属性-CORP\zhangsan”对话框。

02 在“选择页”菜单栏中，选择“服务器角色”选项，显示如图 17.3 所示的“服务器角色”对话框，在“服务器角色”列表中，选择指定用户可以访问的服务器角色。

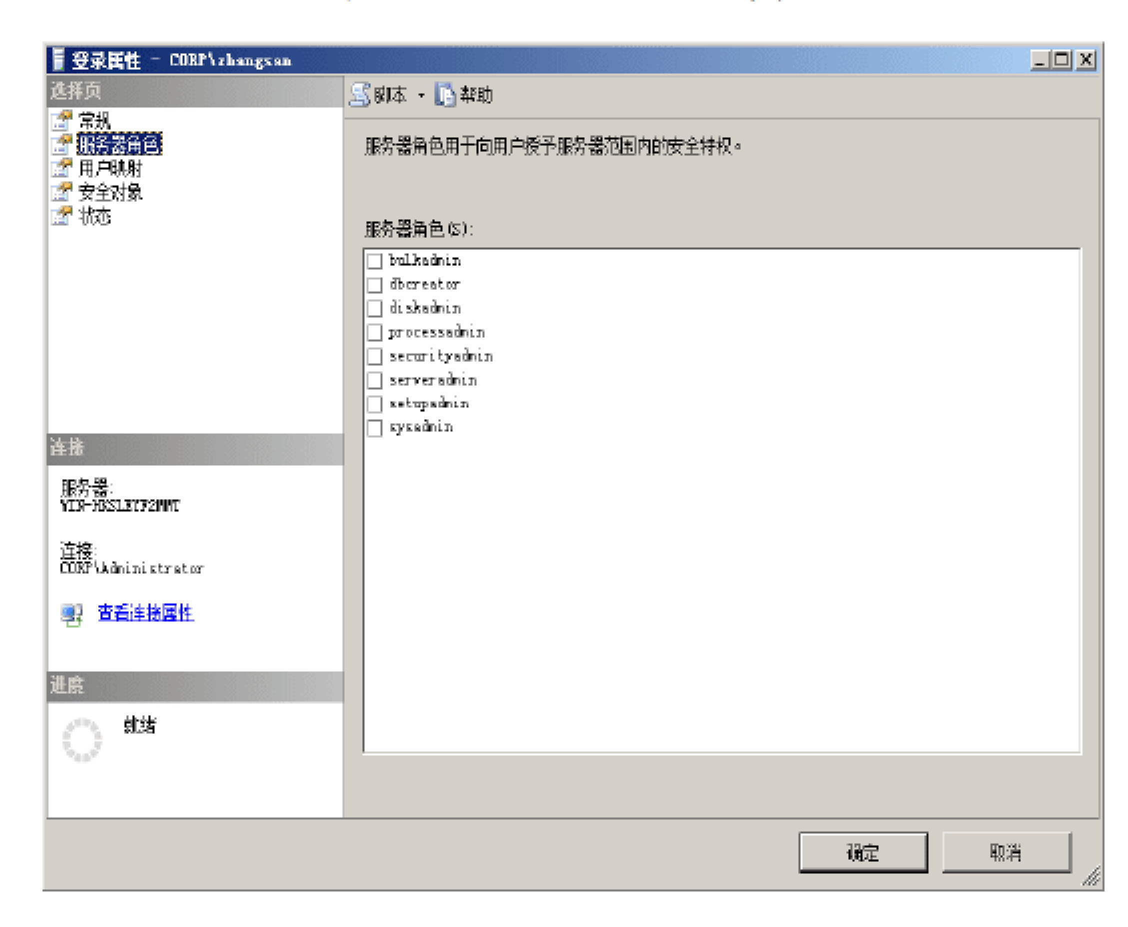


图 17.3　“服务器角色”对话框

03 在“选择页”菜单栏中，选择“用户映射”选项，显示“登录属性-\zhangsan”对话框。选择 zhangsan 可以访问的数据库。在选择某个数据库时，在“数据库角色成员身份”窗口中会显示有效的数据库角色。

04 在“映射到此登录名的用户”列表中选择“master”数据库，单击“默认架构”数据列右侧“…”按钮，显示“选择架构”对话框。

05 单击“浏览”按钮，显示如图 17.4 所示“查找对象”对话框，根据实际情况在“匹配的对象”列表中选中相应的架构复选框。

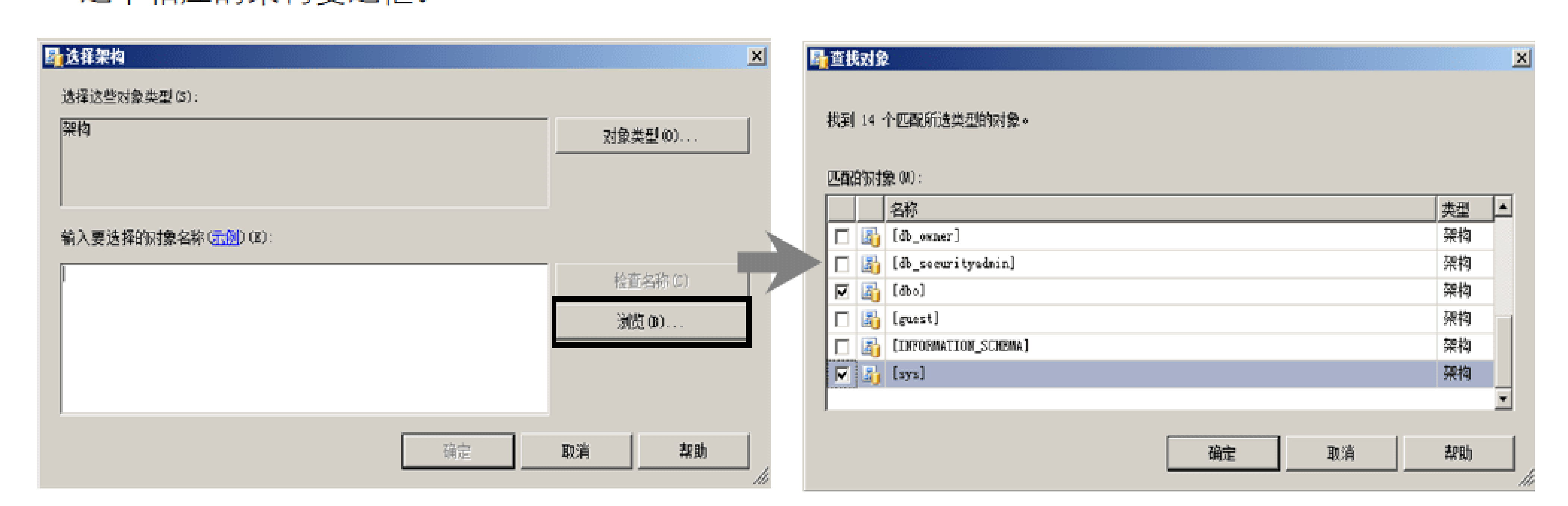


图 17.4　设置匹配的对象

06 单击“确定”按钮，返回“选择架构”对话框。单击“确定”按钮，返回“用户映射”对话框，在“选择页”菜单栏中，单击“安全对象”链接，打开如图 17.5 所示“安全对象”对话框。

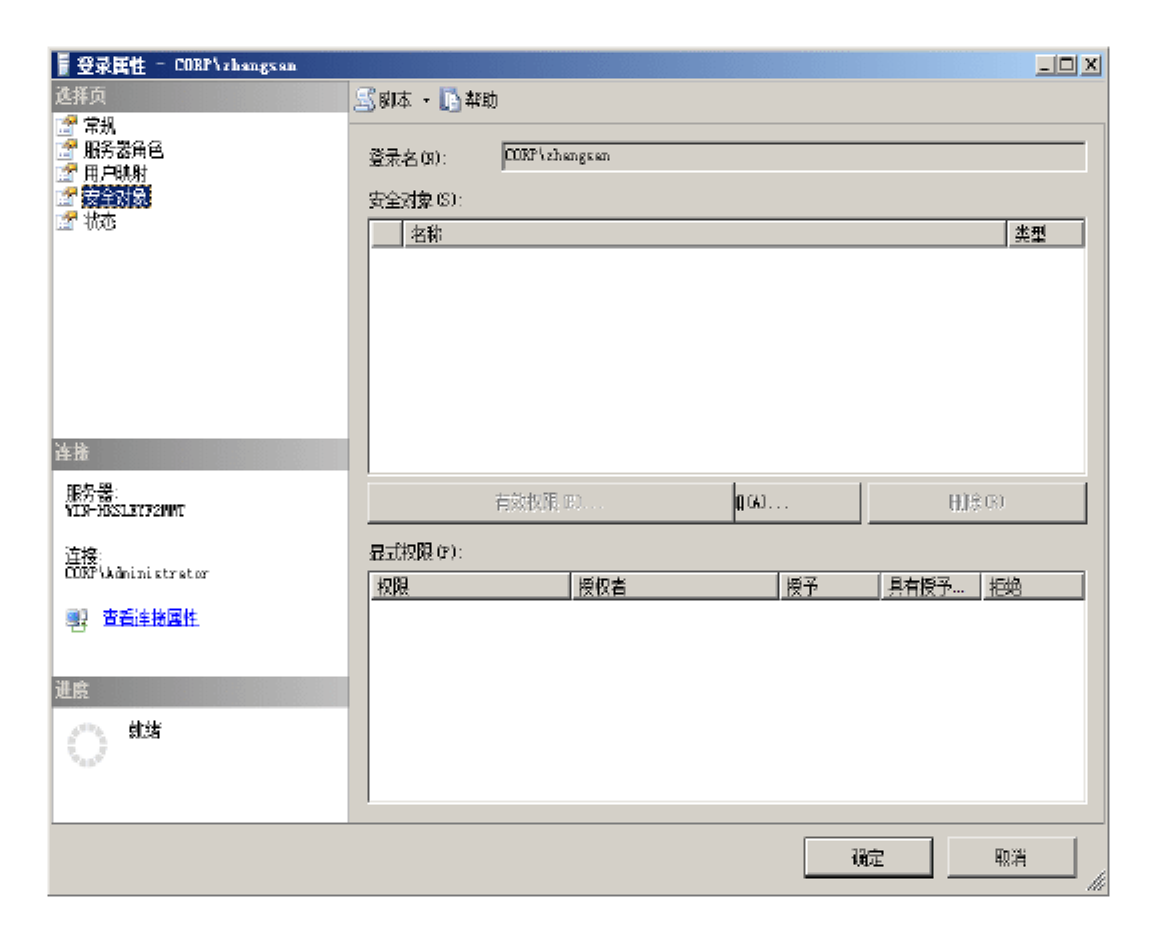


图 17.5 “安全对象”对话框

07 单击“添加”按钮，显示“添加对象”对话框。选择“特定对象”单选按钮，单击“确定”按钮，显示“选择对象”对话框。单击“对象类型”按钮，显示如图 17.6 所示“选择对象类型”对话框，选中“服务器”复选框。

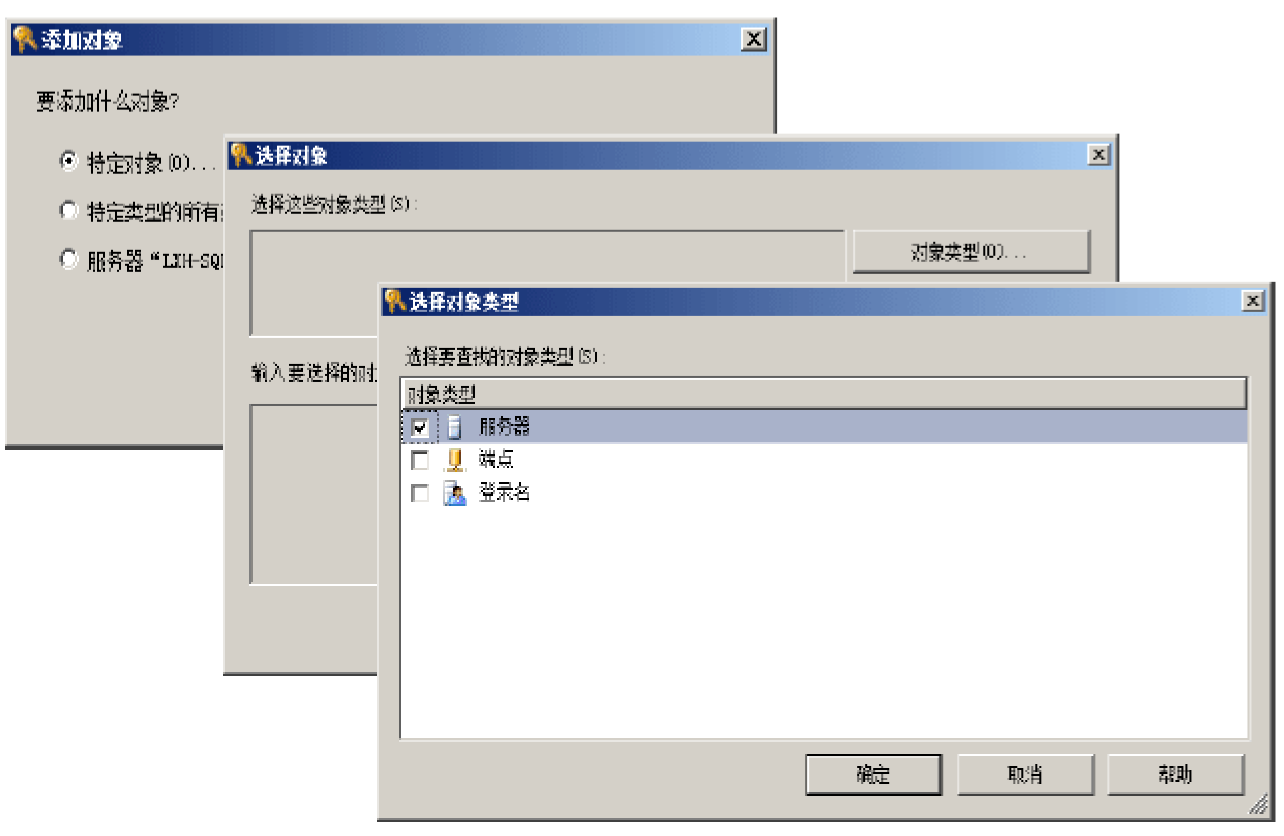


图 17.6 设置安全对象的类型

08 单击“确定”按钮，返回“选择对象”对话框。单击“浏览”按钮，显示如图 17.7 所示“查找对象”对话框，在“匹配的对象”列表中，选中“查找对象”复选框。

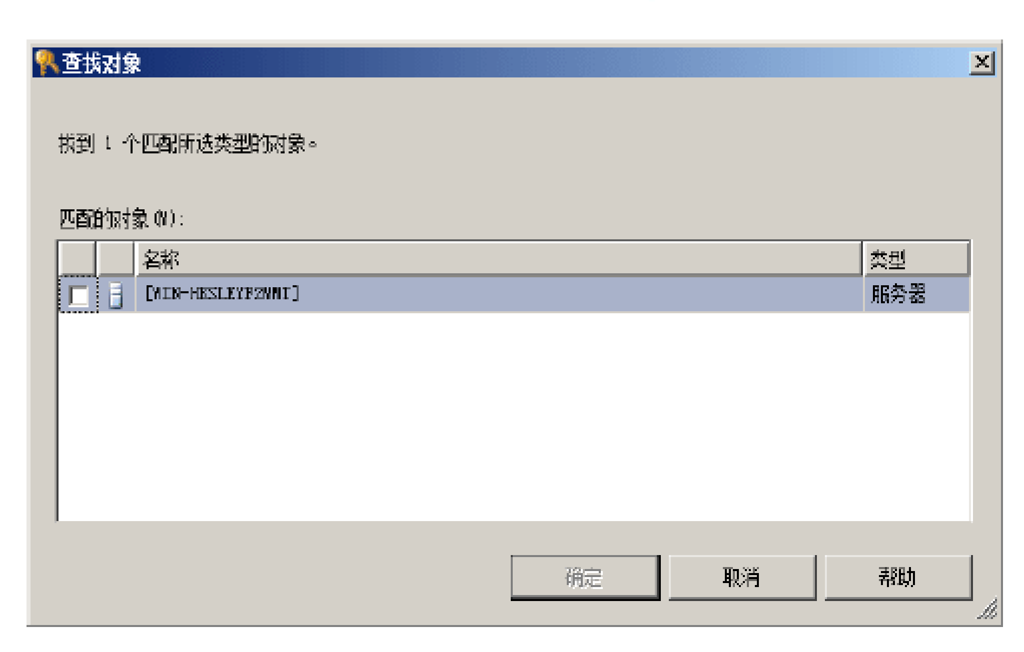


图 17.7 “查找对象”对话框

09 连续单击“确定”按钮，返回“安全对象”对话框。在“WIN-HKSLEYF2MMT 显式权限”列表中，选择给“zhangsan”的相应权限，例如授予 zhangsan 用户“Shutdown”权限，在“Shutdown”选项中，



选中“授予”复选框即可，如图 17.8 所示。

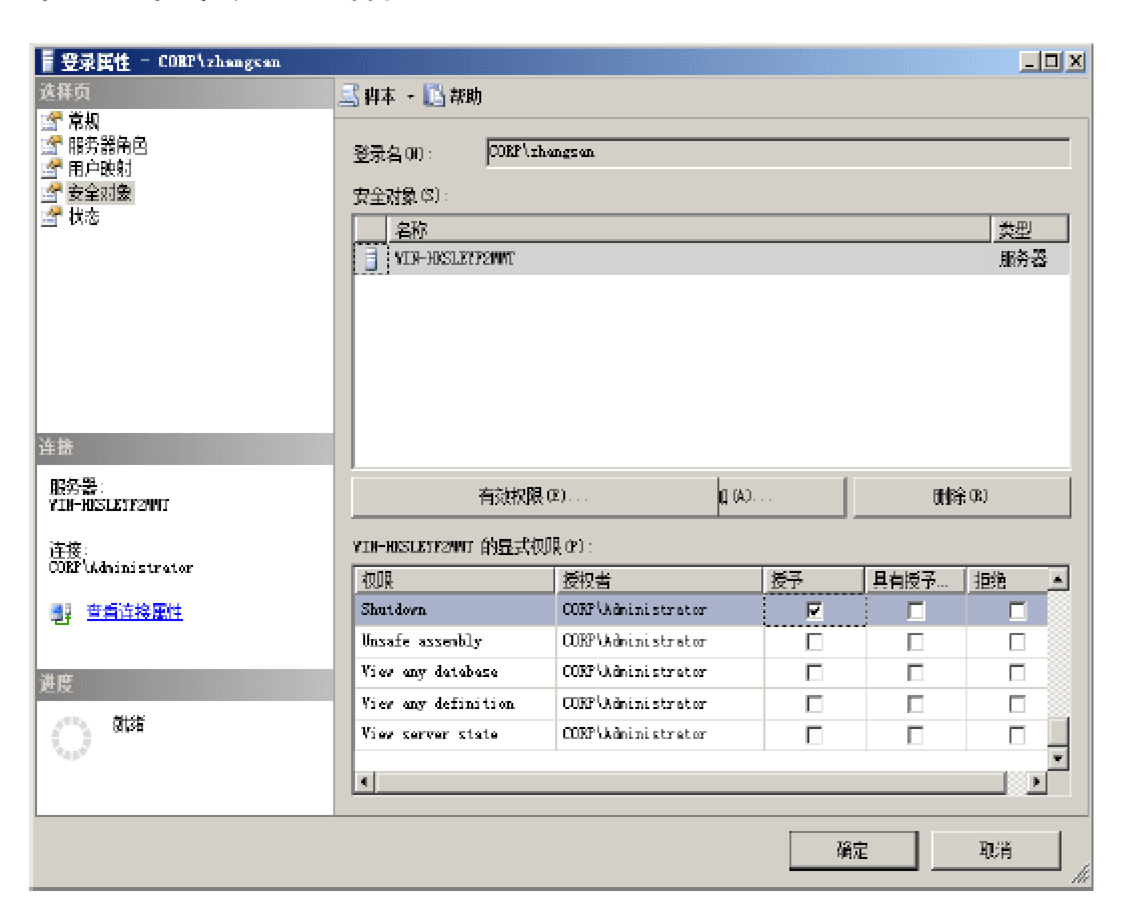


图 17.8　“安全对象”对话框

10 单击“确定”按钮，完成对 zhangsan 用户访问权限的设置。

2. 数据表访问权限设置

用户具备对数据库的访问权限后，管理员可以授予用户对数据表的访问权限，使仅具备访问权限的数据表才可以被用户访问。

01 在“Microsoft SQL Server Management”窗口中，依次选择“WIN-HKSLEYF2MMT”→“数据库”→“master”→“表”，显示“表”窗口。右击需要设置的数据表，在快捷菜单中选择“属性”选项，打开“表属性-company”对话框。在“选择页”菜单栏中，单击“权限”选项。单击“添加”按钮，显示“选择用户和角色”对话框。单击“浏览”按钮，显示如图 17.9 所示“查找对象”对话框，在“匹配的对象”列表中选中登录名“zhangsan”复选框。

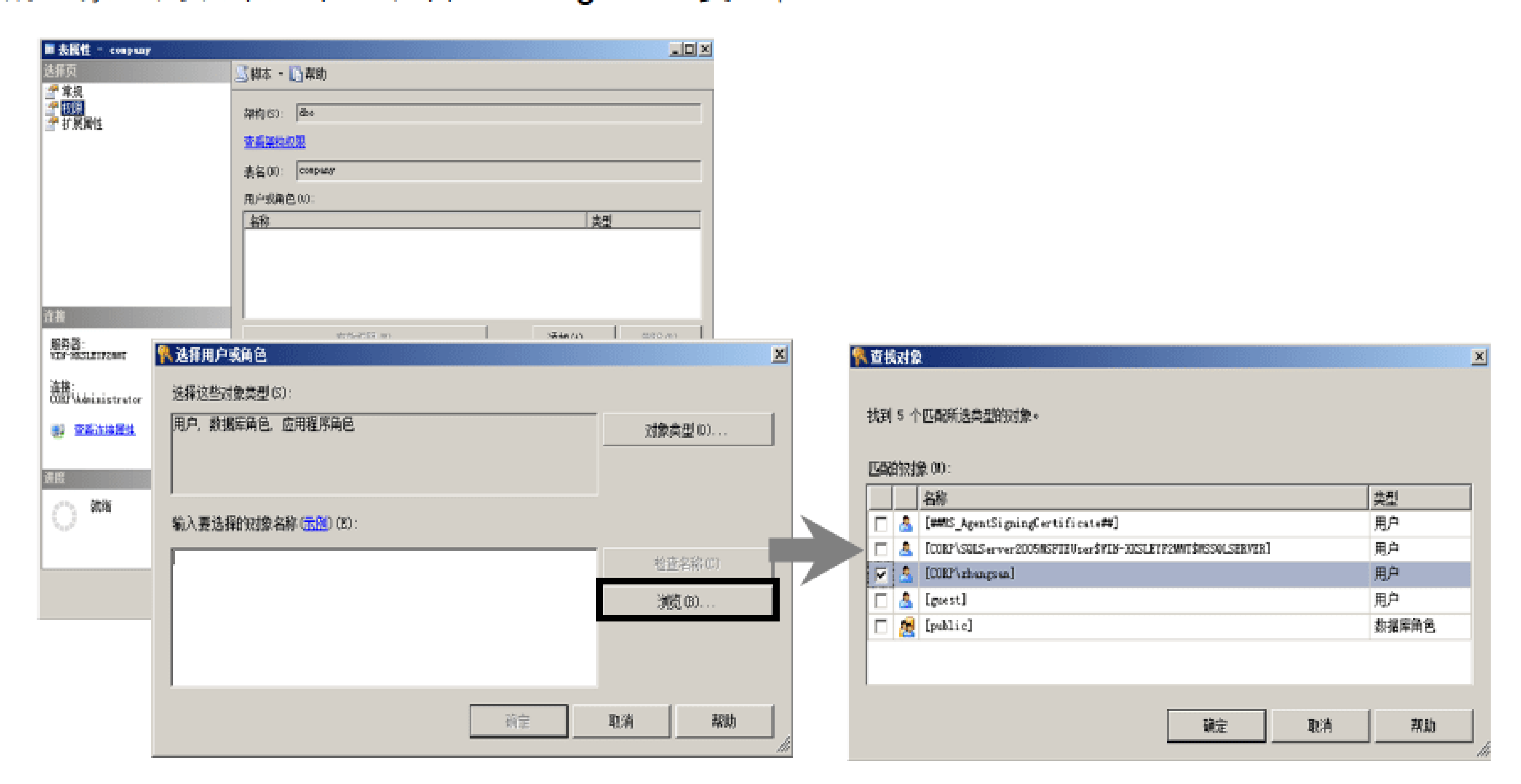


图 17.9　设置授权用户

02 连续单击两次“确定”按钮，返回“权限”对话框。在“zhangsan 的显示权限”列表中，设置用户 zhangsan 对数据表的权限。

03 单击“确定”按钮，完成对用户访问数据表权限的设置。

17.1.3 系统管理员设置

在 SQL Server 2005 中，可以使用 Windows 身份认证和 SQL Server 身份认证两种认证方式登录 SQL。如果不需要系统管理员管理数据库，可以将系统管理员组删除。

1. 删除网络管理员组

01 在“Microsoft SQL Server Management Studio”窗口中，依次选择“WIN-HKSLEYF2MMT”→“安全性”→“登录名”。右击“BUILTIN\Administartor”选项，在快捷菜单中选择“删除”选项，显示如图 17.10 所示“删除对象”对话框。

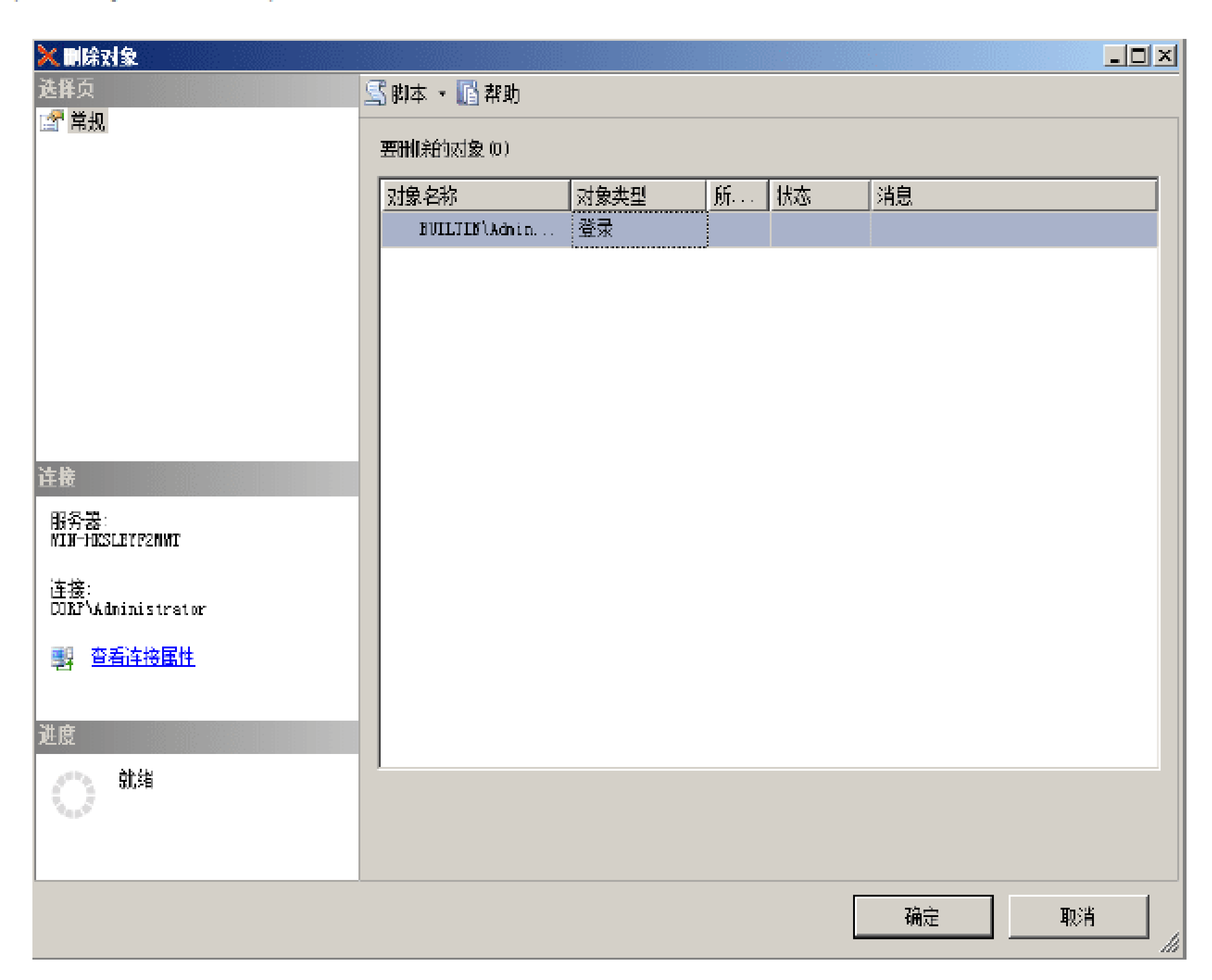


图 17.10 “删除对象”对话框

02 单击“确定”按钮，即可删除“BUILTIN\Administrator”网络管理员组。

2. C2 审核

C2 审核是一个政府安全等级标准，使系统能够保护资源并具有足够的审核能力。管理员通过 C2 审核模式来监视对所有数据库实体的所有访问企图。

01 在“Microsoft SQL Server Management Studio”窗口中，右击“WIN-HKSLEYF2MMT”选项，在快捷菜单中选择“属性”选项，显示如图 17.11 所示“服务器属性 - WIN-HKSLEYF2MMT”对话框。在“选择页”菜单栏中，选择“安全性”选项。



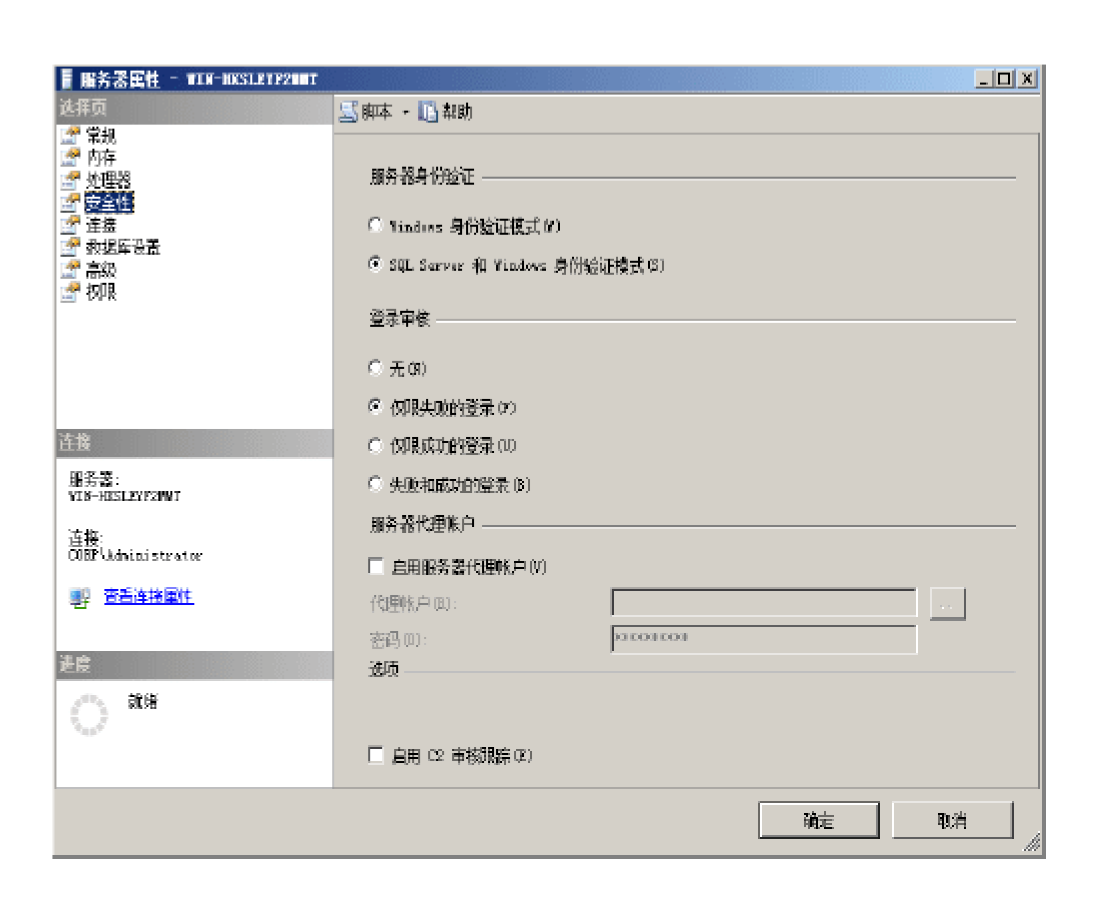


图 17.11　“安全性”对话框

02 在“登录审核”文本域中，选择“失败和成功的登录”单选按钮，同时选中“启用 C2 审核跟踪”复选框。

03 单击“确定”按钮，显示如图 17.12 所示“重启”对话框，单击“确定”按钮即可完成配置。

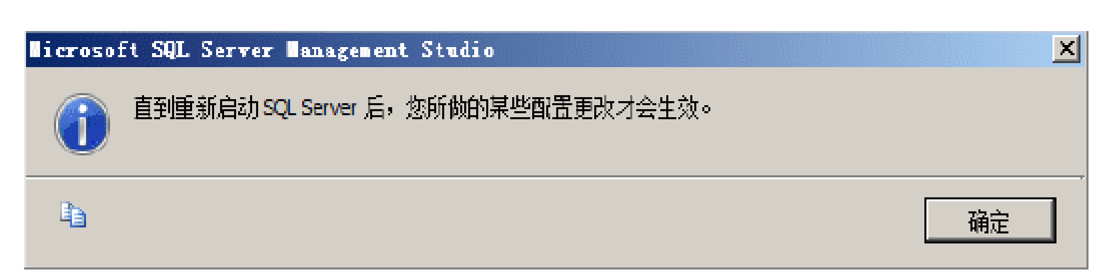


图 17.12　“重启”对话框

> 提示　C2 审核模式将大量事件信息保存在日志文件中，可能会导致日志文件的迅速增大，如果保存日志的数据空间不足，SQL Server 将自动关闭。

3. 修改 SA 帐户名称

SA 帐户是 SQL Server 的内置帐户，其默认的密码为空，管理员应当修改或删除 SA 帐户。

在“Microsoft SQL Server Management Studio”窗口中，依次选择“WIN-HKSLEYF2MMT”→“安全性”→“登录名”。右击“SA”帐户，在快捷菜单中选择“重命名”选项，更改 SA 帐户名，单击“确定”按钮即可完成配置。

17.2　MBSA 数据库扫描

Microsoft 基准安全分析器（Microsoft Baseline Security Analyzer，简称 MBSA），是微软公司提供的一款可以免费下载的安全扫描工具，允许用户扫描一台或多台基于 Windows 的计算机。借助 MBSA，可以扫描 SQL Server 2005 数据库中存在的安全问题，例如，身份验证模式的类型、SA 帐户密码状态和 SQL Server 帐户成员资格。每一次扫描都会记录在安全报告中，并附带有相关修复已发现问题的解决方法。

MBSA 的下载地址是 http://www.microsoft.com/downloads/details.aspx?FamilyID=F32921AF-9DBE-4DCE-889E-ECF997EB18E9&displaylang=en#filelist，这里介绍如何使用 MBSA 扫描 SQL Server 数据库。

01 依次选择“开始”→“所有程序”→“Microsoft Baseline Security Analyzer 2.1”，打开“MBSA”窗口。

02 单击“Scan a computer”超级链接，打开如图 17.13 所示“Which computer do you to scan”窗口。在“Computer name”下拉列表框中，选择需要扫描的计算机，在“Options”选项中选中“Check for SQL Vulnerabilites”复选框。

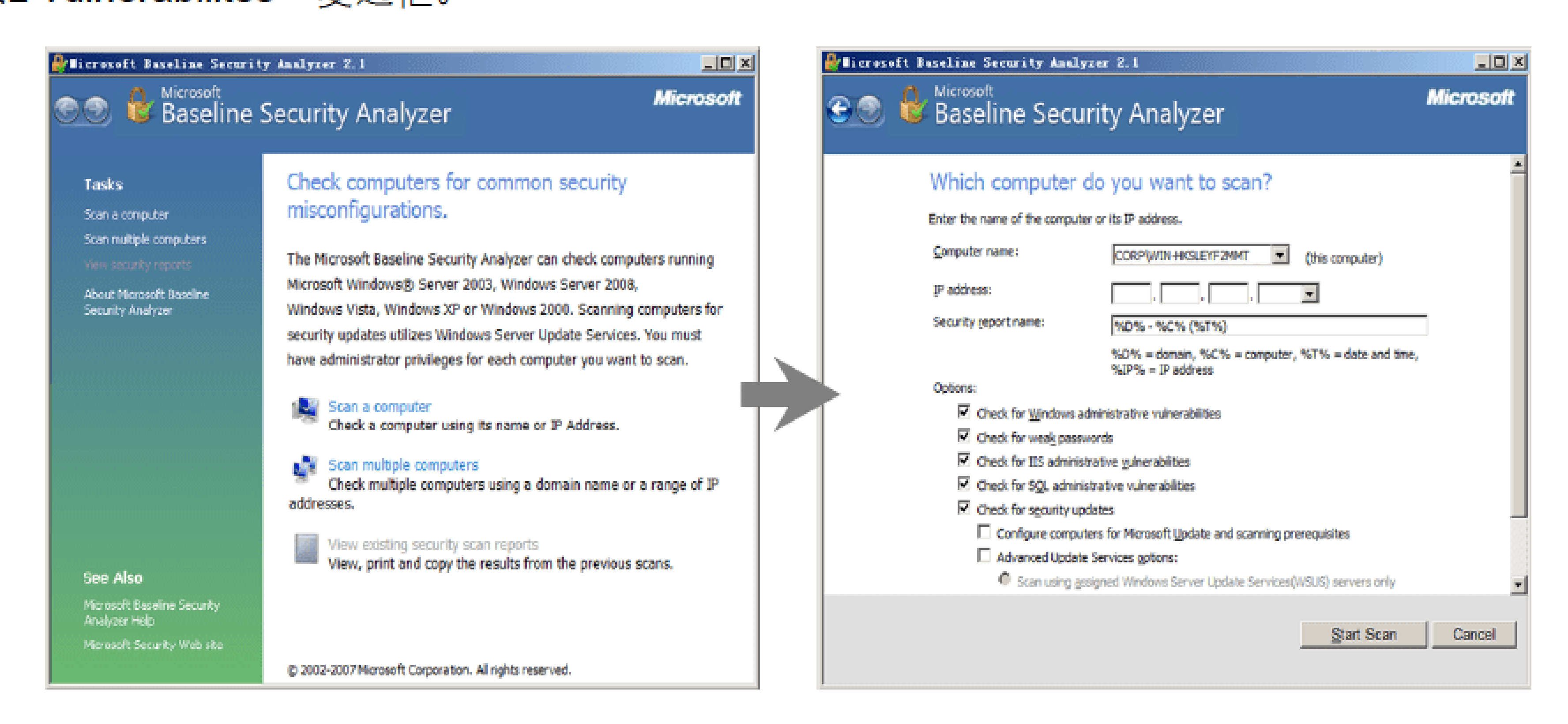
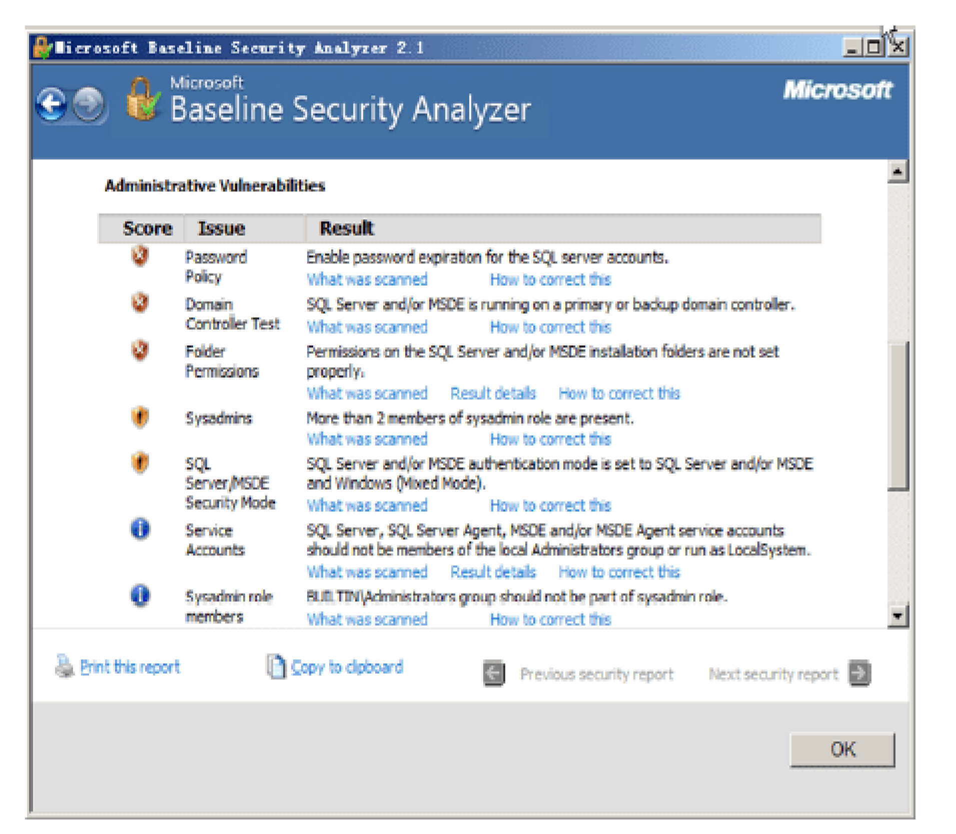


图 17.13 “Which computer do you to scan”窗口

03 单击“Start Scan”按钮，开始扫描，扫描完后自动生成“安全列表”窗口。单击“What was scanned”超级链接，打开如图 17.14 所示的“扫描结果列表”窗口，在窗口中显示了扫描结果及需要采取处理的方案。



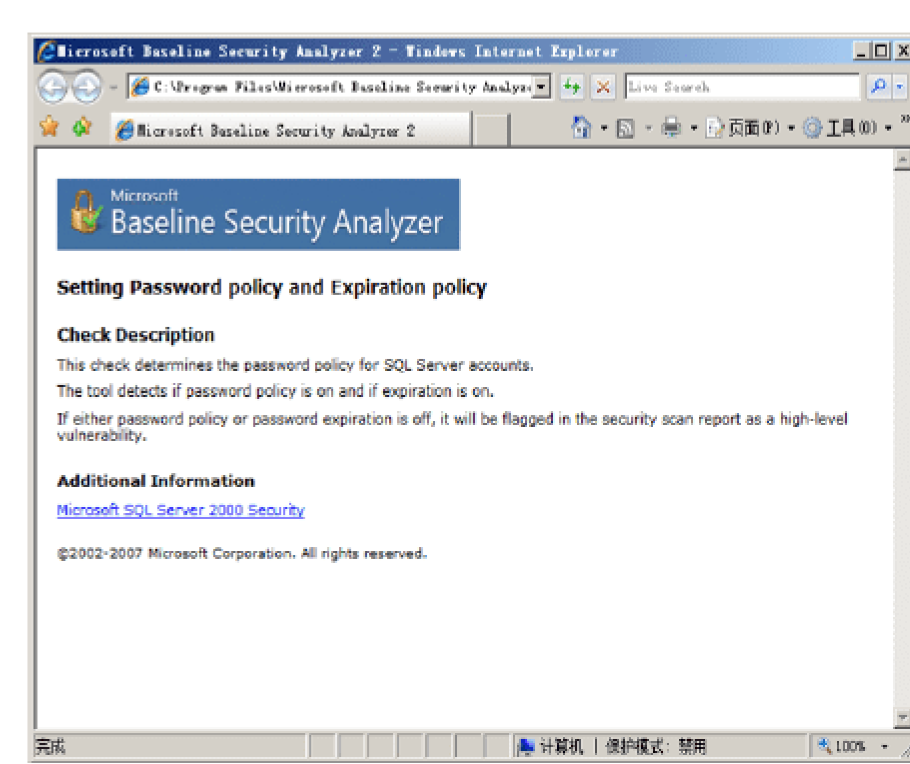


图 17.14 扫描结果

注意



低于 MBSA 2.0.1 的版本不支持 Windows Server 2008 操作系统。

17.3 数据备份与安全

为了防止数据库系统出现灾难性故障，数据库的备份和恢复成了一项必不可少的安全措施。由于数据库更新速度比较频繁，管理员应当定时对数据库进行更新，有些企业甚至采取了实时备份来确保数据的安全性。备份内容包括系统数据库（Master、Msdb、Model、Tempdb、Ddistribution）、用户数据库和事务日志。



17.3.1 数据库的完全备份与恢复

完全备份数据库就是将数据库中的所有数据文件全部复制备份。这种备份方法适合小型数据库，但对于大中型数据库来说，因为数据量比较大，这种备份方式需要花费较多的备份时间和存储空间。

1. 完全备份数据库

完整数据库备份对整个数据库进行备份，包括对部分事务日志进行备份，以便能够恢复完整数据库备份。

01 在“Microsoft SQL Server Management Studio”窗口中，选择“数据库”选项，在“数据库”中选择需要备份的数据库对象，例如 company，右击“company”，在快捷菜单中依次选择“任务”→“备份”，打开如图 17.15 所示的“备份数据库 - company”对话框。

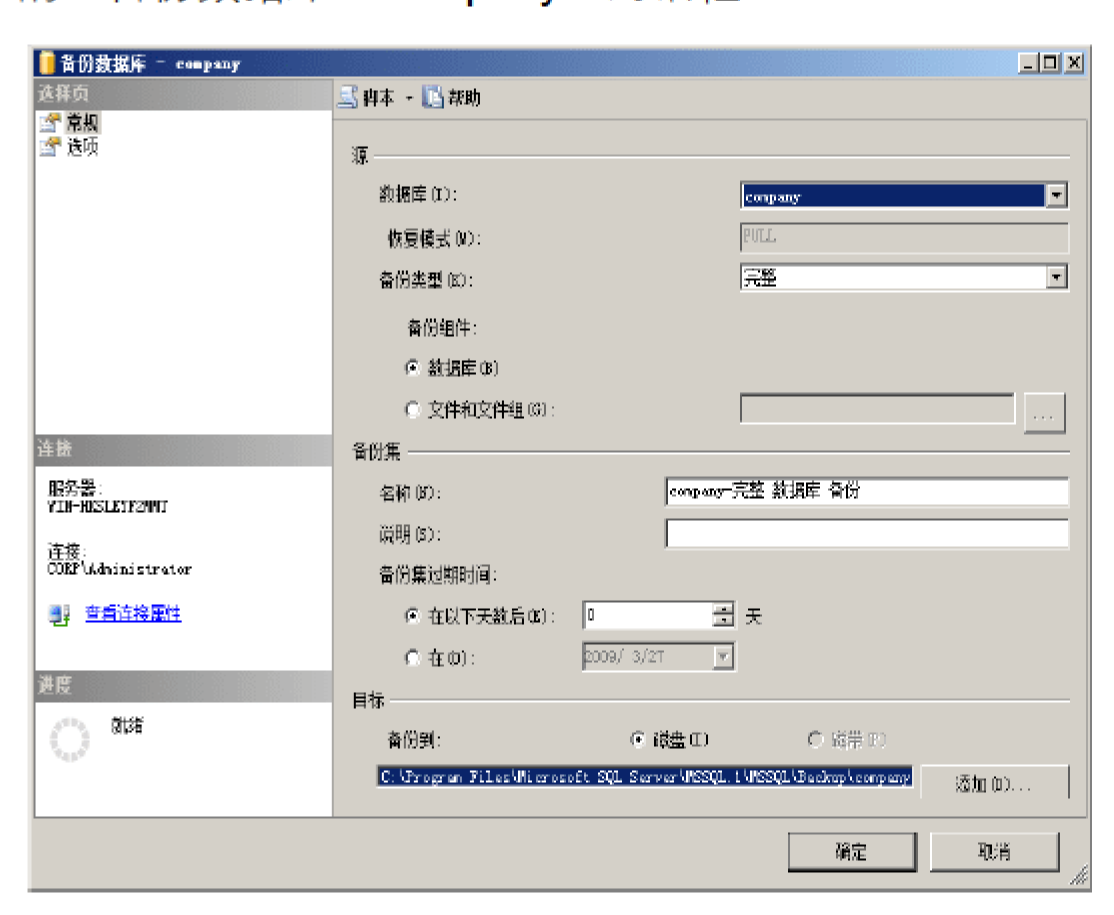


图 17.15 “备份数据库 - company”对话框

02 在“源”文本域中，在“备份类型”下拉列表中选择“完整”选项，在“备份组件”文本域中选择“数据库”单选按钮，在“备份集”文本域中填写备份数据的名称和相关说明，在“备份集过期时间”中选择备份集过期的时间，如果时间设为 0，表示始终不过期。

03 在“目标”文本区域中，选择数据库备份存储的地方，可以选择磁盘或磁带，单击“添加”按钮，打开“选择备份目标”对话框。在“文件名”文本框中输入备份文件存放的目标文件夹。

04 单击“确定”按钮，开始备份数据库，数据库备份完成后显示如图 17.16 所示“备份完成”对话框。



图 17.16 “备份完成”对话框

2. 完全恢复数据库

01 在“Microsoft SQL Server Management Studio”窗口中，选择“数据库”选项，选择想要恢复的数据

库对象，右击“数据库名”，在快捷菜单中依次选择“任务”→“还原”→“数据库”，打开如图 17.17 所示的“还原数据库”对话框。

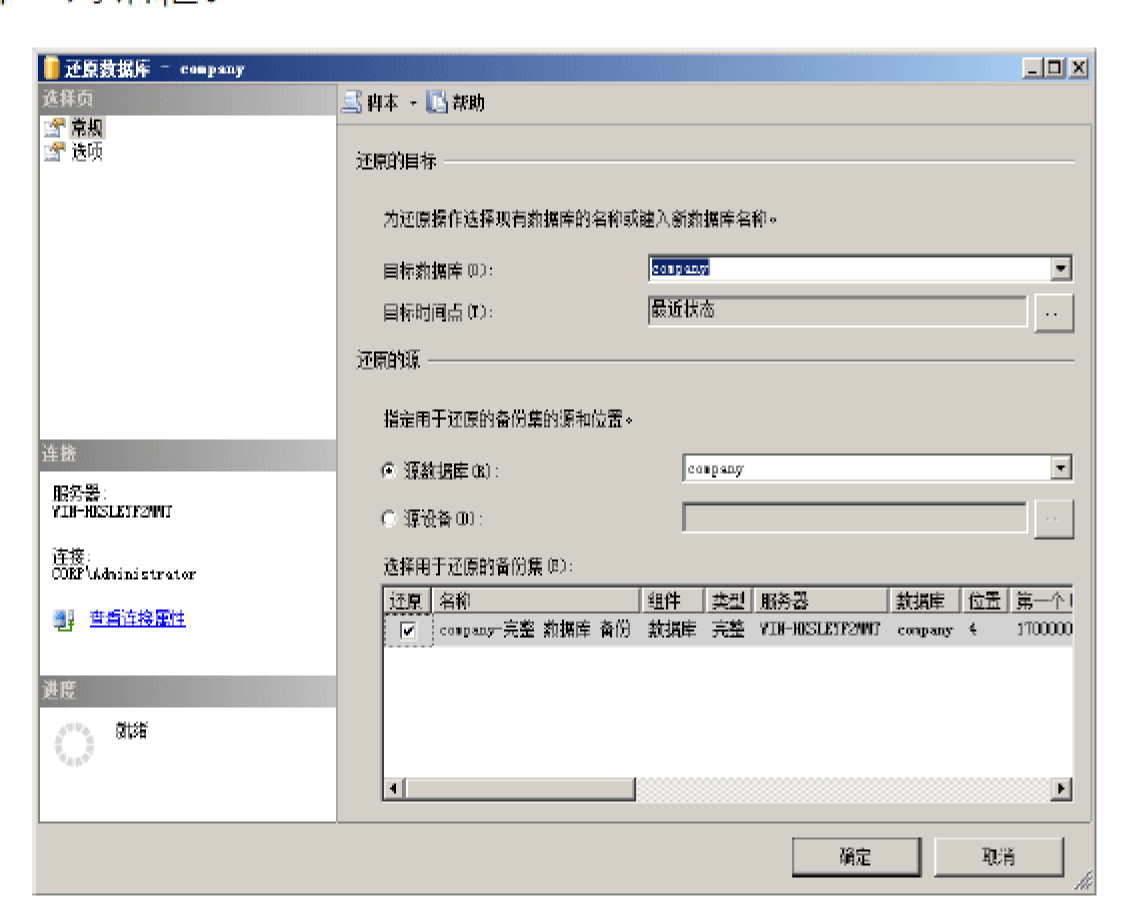


图 17.17 “还原数据库”对话框

02 在“还原的目标”文本域中，选择“目标数据库”的名称和“目标时间”，在“还原的源”文本域中，选择指定用于还原的备份集和位置，选择“源设备”单选按钮，单击“...”按钮，显示“指定备份”对话框。单击“添加”按钮，显示如图 17.18 所示“定位备份文件”对话框，根据实际需要，选择备份的数据库文件。

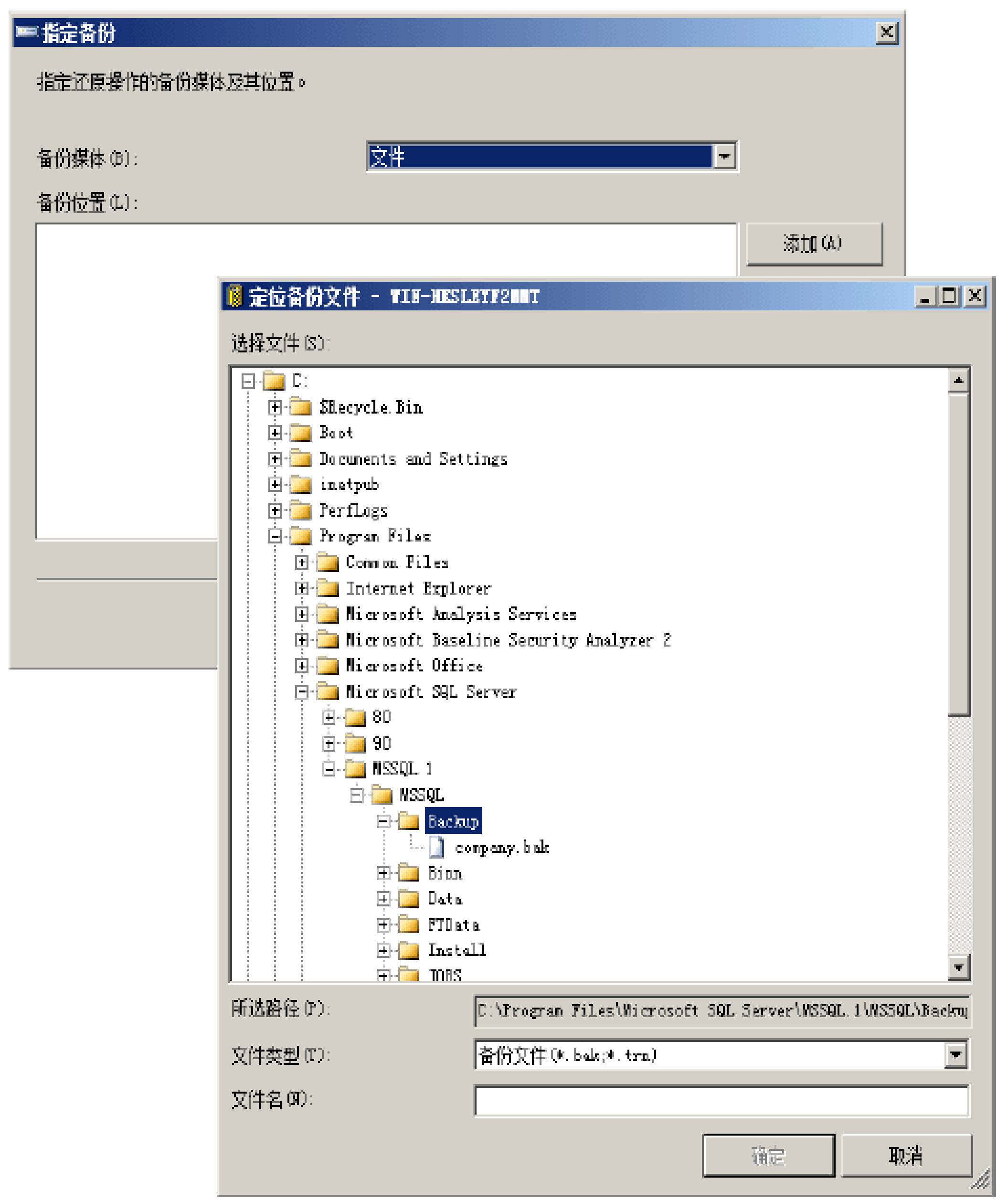


图 17.18 指定备份文件

03 连续单击“确定”按钮，返回到“还原数据库”对话框。在“选择用户还原的备份集”文本域中，选中需要还原的备份文件，在左侧“选择页”菜单栏中选择“选项”选项，显示如图 17.19 所示“选项”对话框。在“还原选项”文本域中选择合适的还原方式，包括如下四种还原方式：

■ 覆盖现有数据库；



- 保留复制设置；
- 还原每个备份之前进行提示；
- 限制访问还原的数据库。

04 在“将数据库还原为”文本域中，单击“...”按钮，显示如图 17.20 所示“定位数据库文件 -WIN-HKSLEYF2MMT”对话框，选择指定的目标文件夹。

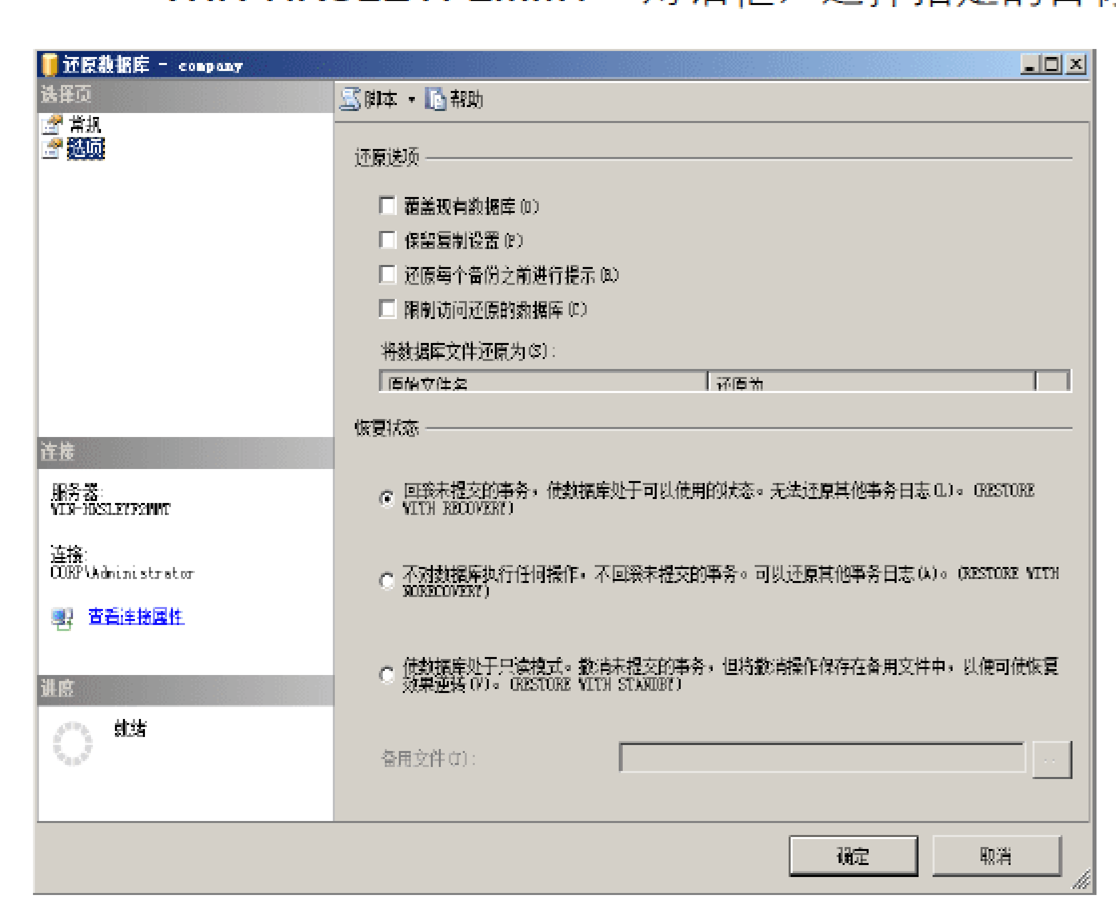


图 17.19　“选项”对话框

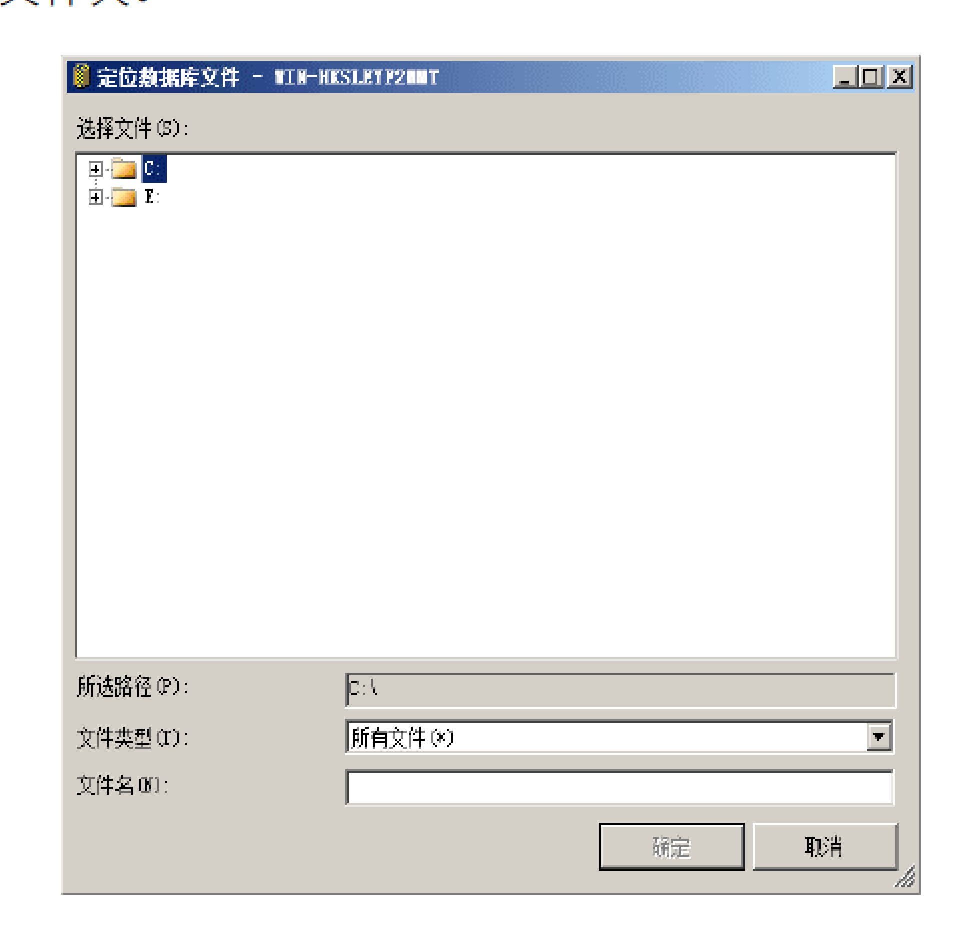


图 17.20　“定位数据库文件 - WIN-HKSLEYF2MMT”对话框

05 在“恢复状态”文本域中，设置数据库的恢复状态，包括如下三种选项：

- 回滚未提交的事务，使数据库处于可以使用的状态。无法还原其他事务日志；
- 不对数据库执行任何操作，不回滚未提交的事务，可以还原其他事务日志；
- 使数据库处于只读模式。撤消未提交的事务，但将撤消操作保存在备用文件中，以便可使恢复效果逆转。

06 单击“确定”按钮，开始执行还原操作，数据恢复完成后显示“还原成功”对话框，单击“确定”按钮，关闭向导即可。

17.3.2　数据库的差异备份与恢复

相对于完全备份数据库，差异备份非常适合大中型数据库，备份效率非常高。所谓差异备份，只备份与已经备份的数据不同的数据，而相同的数据则不进行备份。

1. 差异备份数据库

“差异数据库备份”只记录自上次完整数据库备份后更改的数据。此完整备份称为“差异基准”。差异数据库备份比完整数据库备份更小、更快。这会缩短备份时间，但将增加复杂程度。对于大型数据库，差异备份的间隔可以比完整数据库备份的间隔更短。这将降低工作丢失风险。

01 在“MicrosoftSQL Server Management Studio”窗口中，依次选择“WIN-HKSLEYF2MMT”→“数据库”，右击“company”并在快捷菜单中依次选择“任务”→“备份”，显示如图 17.21 所示“备份数据

库 - company”对话框。在“备份模式”下拉列表中选中“差异”选项，选择“数据库”单选按钮，其他设置保持默认设置即可。

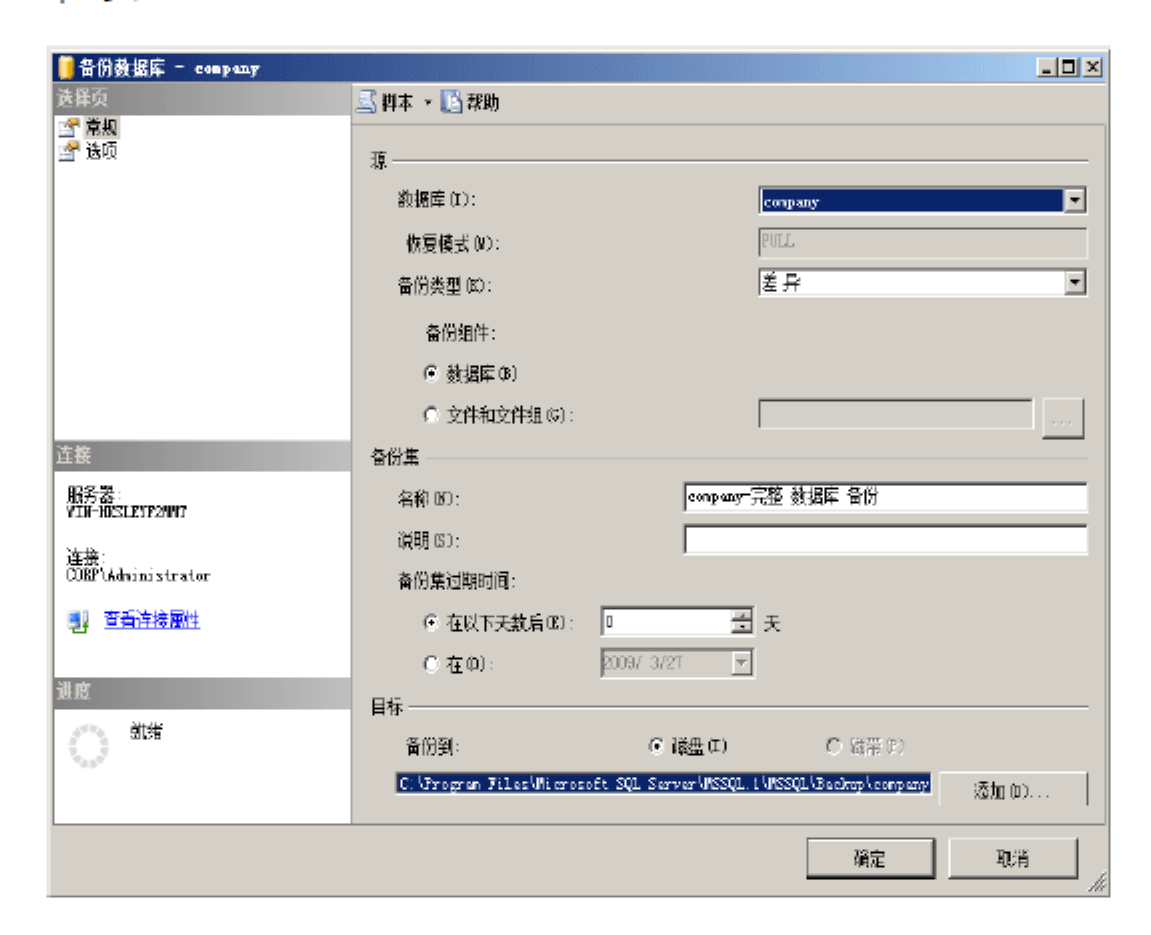


图 17.21 “备份数据库 - company”对话框

02 单击“确定”按钮，备份完后显示“备份成功”的对话框，单击“确定”按钮即可。

注意



备份数据库需要完成 2 部分的备份，首先需完成完全数据库备份，然后完成差异数据库备份。

2. 还原差异备份

在恢复差异备份时，必须恢复最后一次的完整备份。

01 在“Microsoft SQL Server Management Studio”窗口中，依次选择“WIN-HKSLEYF2MMT”→“数据库”，右击“company”并在快捷菜单中依次选择“任务”→“还原”→“数据库”，显示如图 17.22 所示“还原数据库 - company”对话框。在“目标数据库”下拉列表中，选择需还原的数据库，选择“源数据库”单选按钮，在“源数据库”下拉列表中选择源数据库，在“选择用户还原的备份集”文本框中，选中还原的备份集。

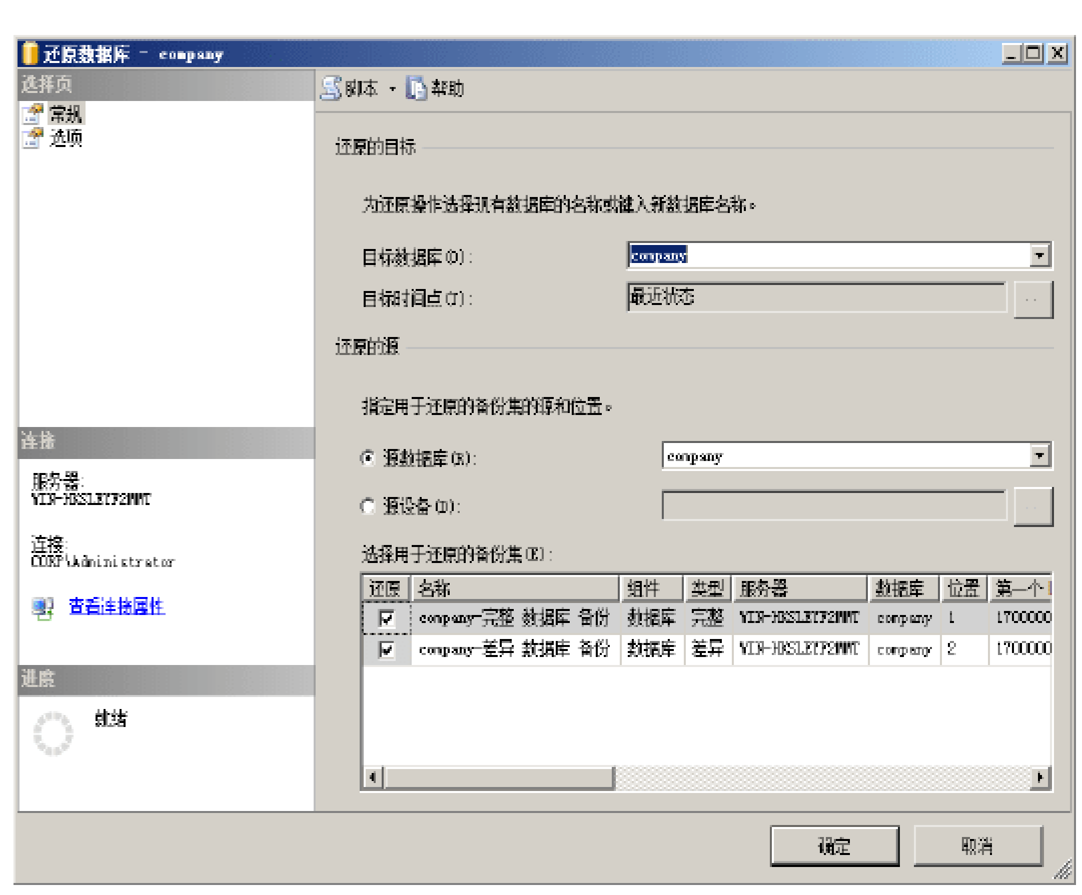


图 17.22 “还原数据库 - company”对话框



02 单击“确定”按钮，开始还原。还原完成后，显示“还原成功”对话框，单击“确定”按钮即可。



注意　恢复差异数据库跟备份差异数据库一样，首先需要恢复完全数据库备份，然后才可以恢复差异数据库备份。

17.3.3　事务日志备份与还原

对事务日志的备份与还原，可以采用作业模式来减轻管理负担，提高作业效率。下面介绍使用备份设备来存储事务日志的方法。

1. 创建事务日志备份

在完整恢复模式和大容量日志恢复模式下，执行例行事务日志备份对于恢复数据十分必要。

01 在“Microsoft SQL Server Management Studio”窗口中，依次选择“WIN-HKSLEYF2MMT”→“服务器对象”，右击“备份设备”选项，在快捷菜单中选择“新建备份设备”选项，打开“备份设备”对话框。在“设备名称”文本框中，输入设备名称，在“目标”文本区域中，选中“文件”单选按钮。

02 单击“...”按钮，显示如图 17.23 所示“定位数据库文件”对话框，在“选择文件”列表中选择目标文件。

03 连续单击两次“确定”按钮，返回“备份设备”对话框，完成备份设备的创建。

04 展开“数据库”，右击“company”并在快捷菜单中依次选择“任务”→“备份”，显示“备份数据库-company”对话框。在“数据库”文本框下拉列表中选择“company”选项，在“备份类型”下拉列表中选择“事务日志”选项。

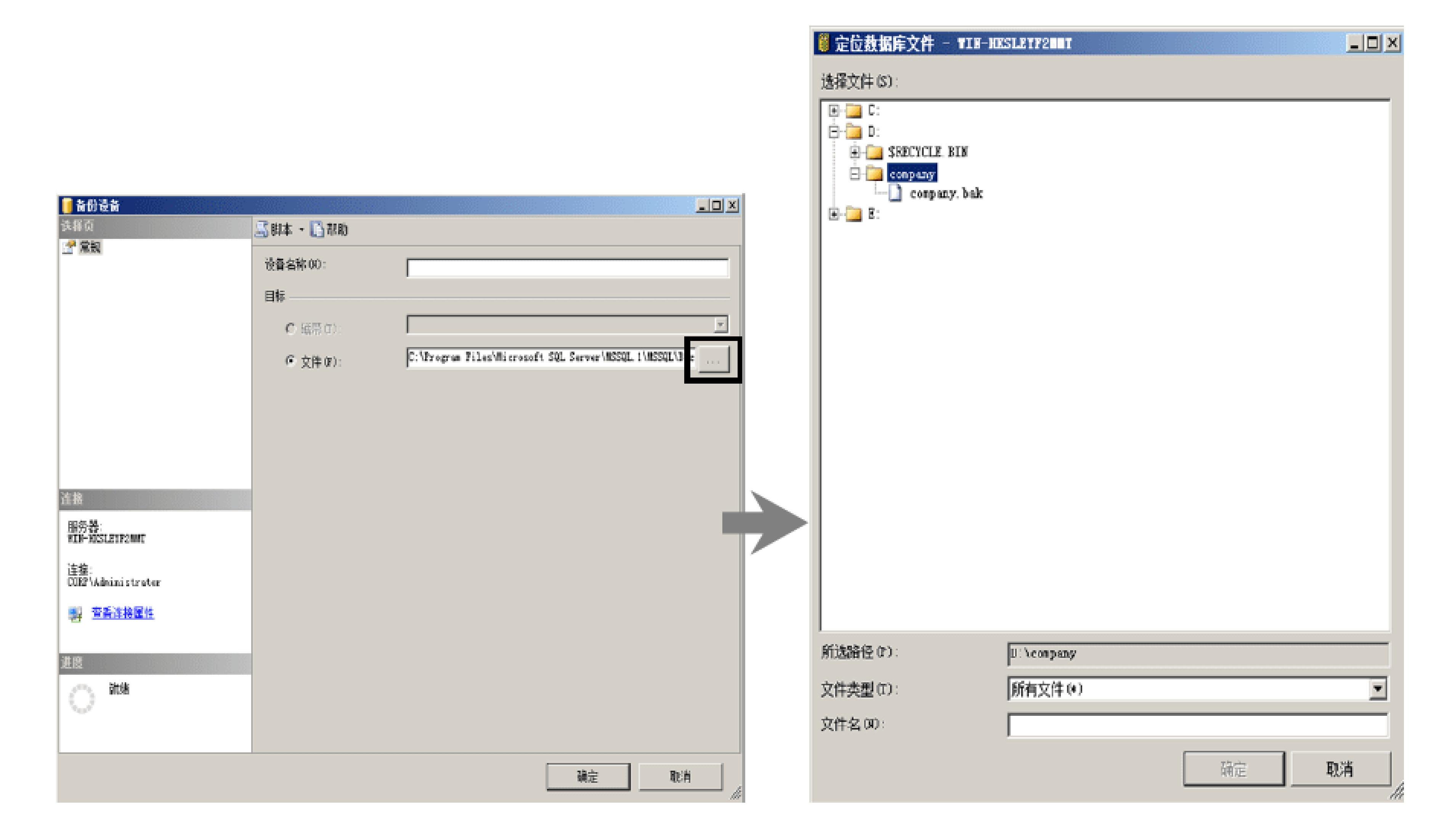


图 17.23　打开“定位数据库文件”对话框

05 在“目标”文本区中，单击“添加”按钮，显示如图 17.24 所示“选择备份目标”对话框。选择“备份设备”单选按钮，在下拉列表框中选中“company”选项，单击“确定”按钮，返回“备份数据库 - company”对话框。

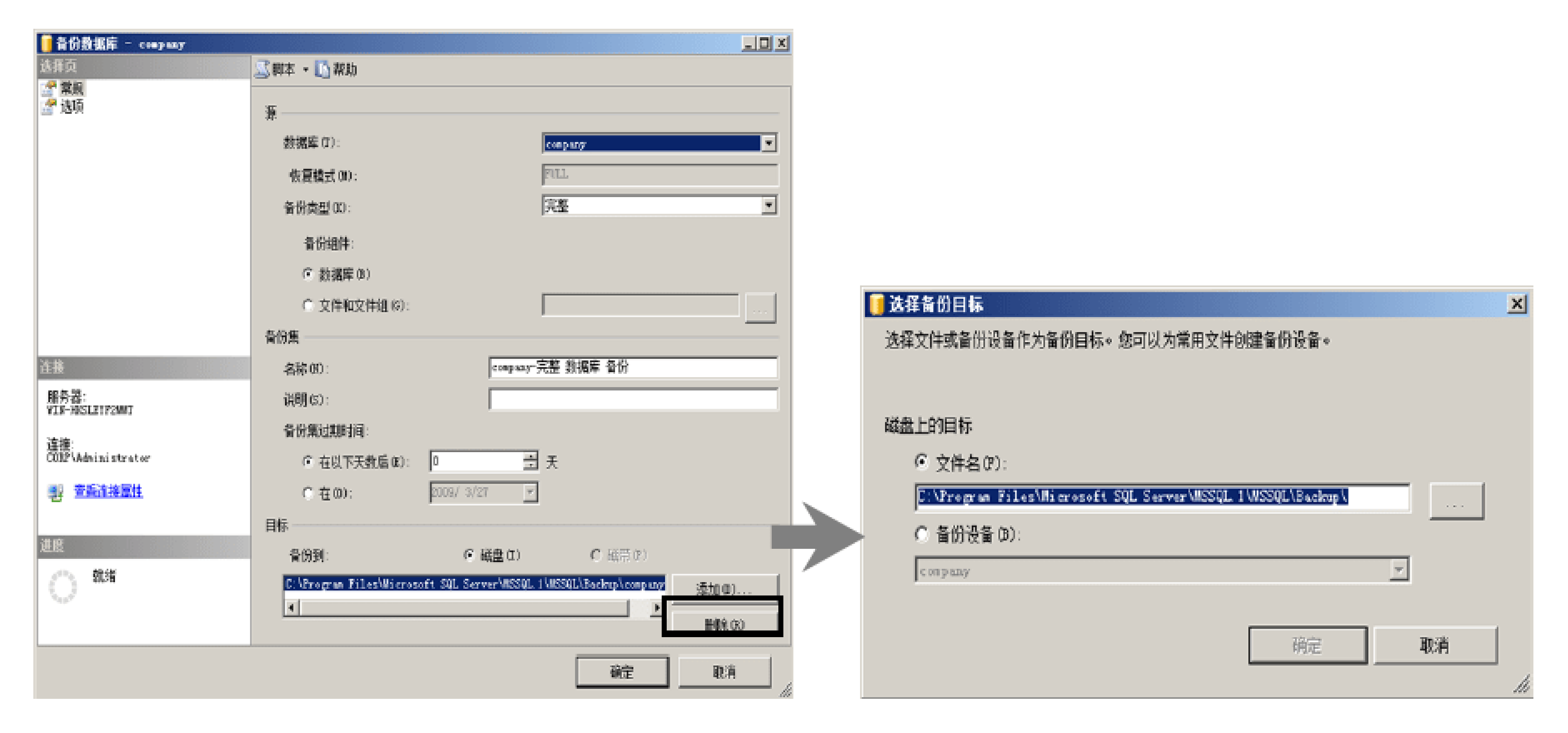


图 17.24　选择备份目标

06 单击“确定”按钮，显示如图 17.25 所示“备份成功”对话框，事务日志备份成功。



图 17.25　“备份成功”对话框

2. 还原事务日志备份

还原事务日志备份，可以对重要数据进行恢复。

01 在“Microsoft SQL Server Management Studio”窗口中，右击“数据库”选项，在快捷菜单中选择“还原数据库”选项，显示如图 17.26 所示“还原数据库-”对话框。

02 在“目标数据库”下拉列表框中，选择需要还原的数据库（以 company 为例），选中“company”选项，选中“源设备”单选按钮，单击“...”按钮，显示“指定设备”对话框。在“备份媒体”下拉列表中选中“备份设备”选项，单击“添加”按钮，显示如图 17.27 所示“选择备份设备”对话框。在“备份设备”下拉列表中，选择“company”选项。

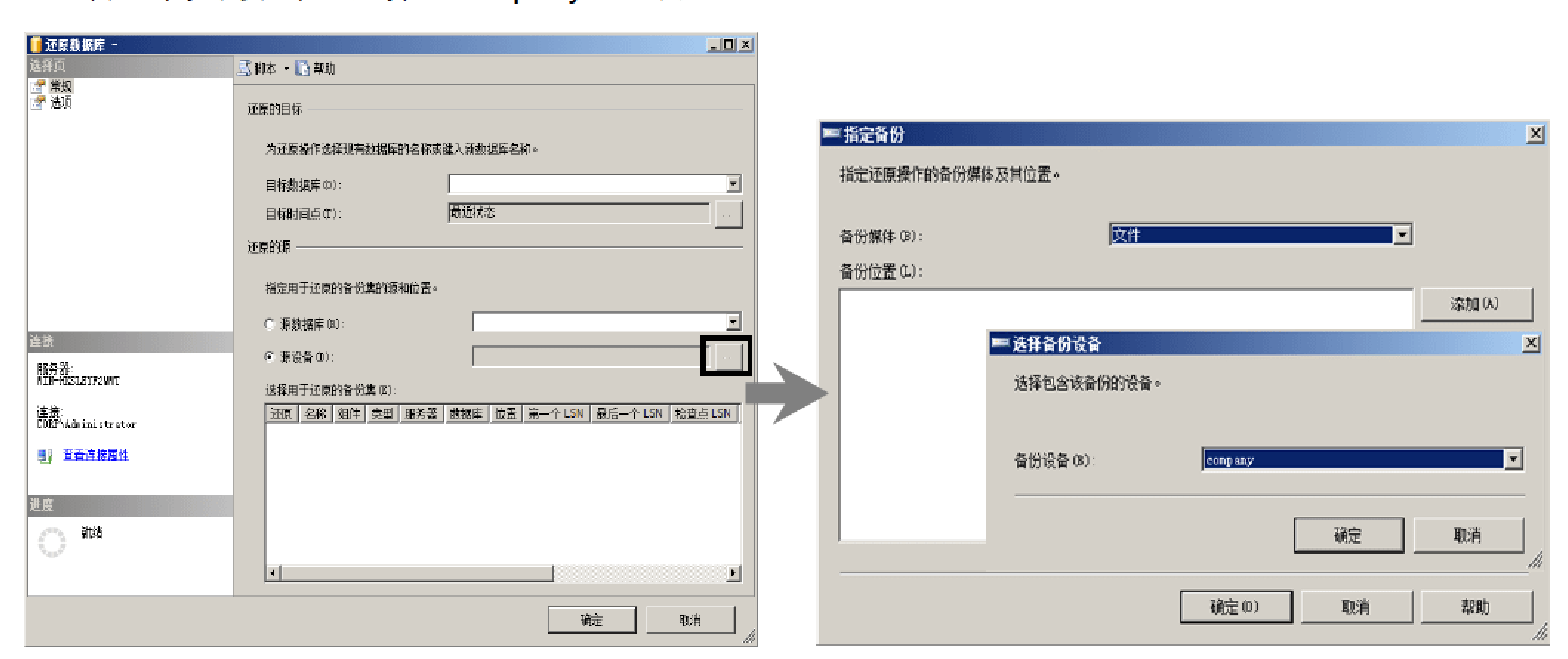


图 17.26　“还原数据库-”对话框　　　图 17.27　“选择备份设备”对话框



03 连续单击两次“确定”按钮，返回“还原数据库 - company”对话框。在“选择用户还原的备份集”列表中，列出了备份设备中包含的所有备份文件，选择需要还原的事务日志文件。

04 在“选择页”菜单栏中，选中“选项”选项，在“恢复状态”文本区域中，设置数据库的恢复状态。

05 单击“确定”按钮，显示“还原成功”对话框，单击“确定”按钮，完成对事务日志的还原。

> 注意
> 要还原事务日志，首选要还原备份数据库，并将数据库置于“还原”状态。

17.3.4　文件和文件组备份与还原

文件和文件组备份是指对数据库文件或文件夹进行备份，但不对事务日志备份。使用此方法可以提高数据库备份和还原的速度。这里以 company 数据库为例对文件和文件组进行备份与还原。

1. 文件和文件组备份

当数据库大小和性能要求使完整数据库备份显得不切实际，则可以创建文件备份。“文件备份”包含一个或多个文件（或文件组）中的所有数据。

01 在“Microsoft SQL Server Management Studio”窗口中，选择“数据库”选项，右击“company”并在快捷菜单中依次选择“任务”→“备份”，显示如图 17.28 所示的“备份数据库 - company”对话框。

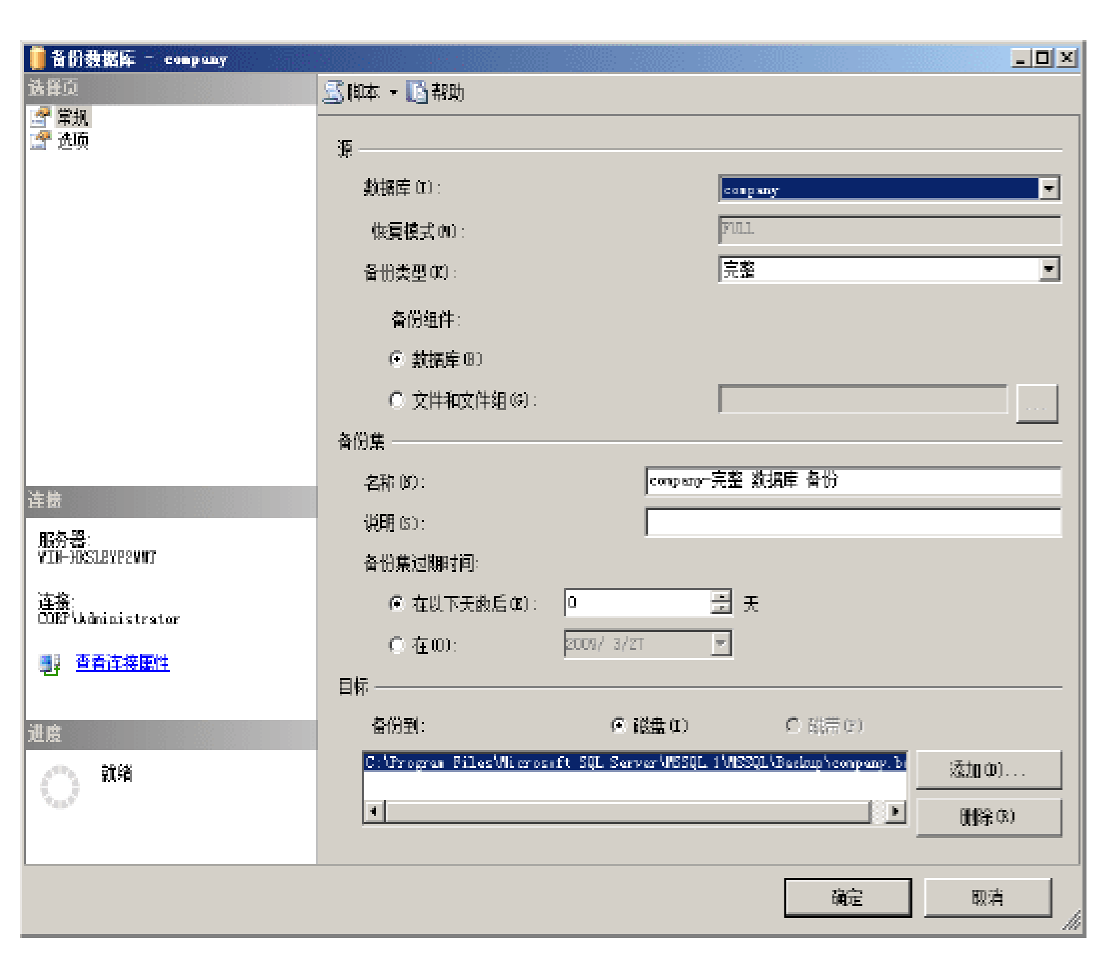


图 17.28　“备份数据库 - company”对话框

02 在“数据库”下拉列表中选中“company”选项，在“备份类型”下拉列表中选择“完整”选项，在“备份组件”文本域中选择“文件和文件组”单选按钮，显示如图 17.29 所示“选择文件和文件组”对话框，选中“company”复选框。

03 单击“确定”，返回“备份数据库 - company”对话框。在“目标”文本域中，单击“添加”按钮，显示如图 17.30 所示“选择备份目标”对话框。



图 17.29 “选择文件和文件组”对话框

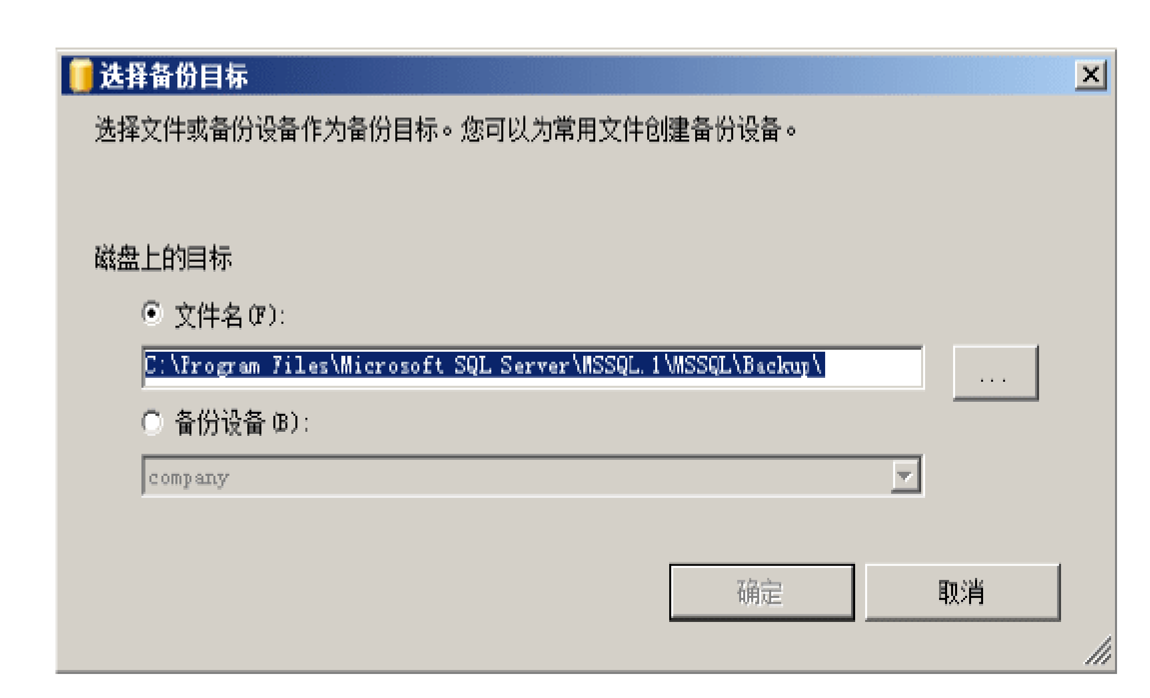


图 17.30 “选择备份目标”对话框

04 单击“...”按钮，显示“定位数据库文件 - WIN-HKSLEYF2MMT”对话框，选择“备份设备”单选按钮，在备份设备下拉列表中选中“company”选项，单击“确定”按钮，返回“备份数据库 - company”对话框，显示如图 17.31 所示“备份成功”对话框，单击“确定”按钮即可。



图 17.31 “备份成功”对话框

2. 还原文件和文件组

文件和文件组备份仅可以还原到其所属的数据库，不能使用相同的结构和文件名创建新的空白数据库，并尝试还原单个文件组备份；必须将其还原到现有数据库，或在其他位置执行完整数据库还原。

01 在“SQL Server Management Studio”中，选择“数据库”选项，右击“company”，并在快捷菜单中依次选择“任务”→“还原”→“文件和文件组”，打开“还原文件和文件组 - company”对话框，如图 17.32 所示。

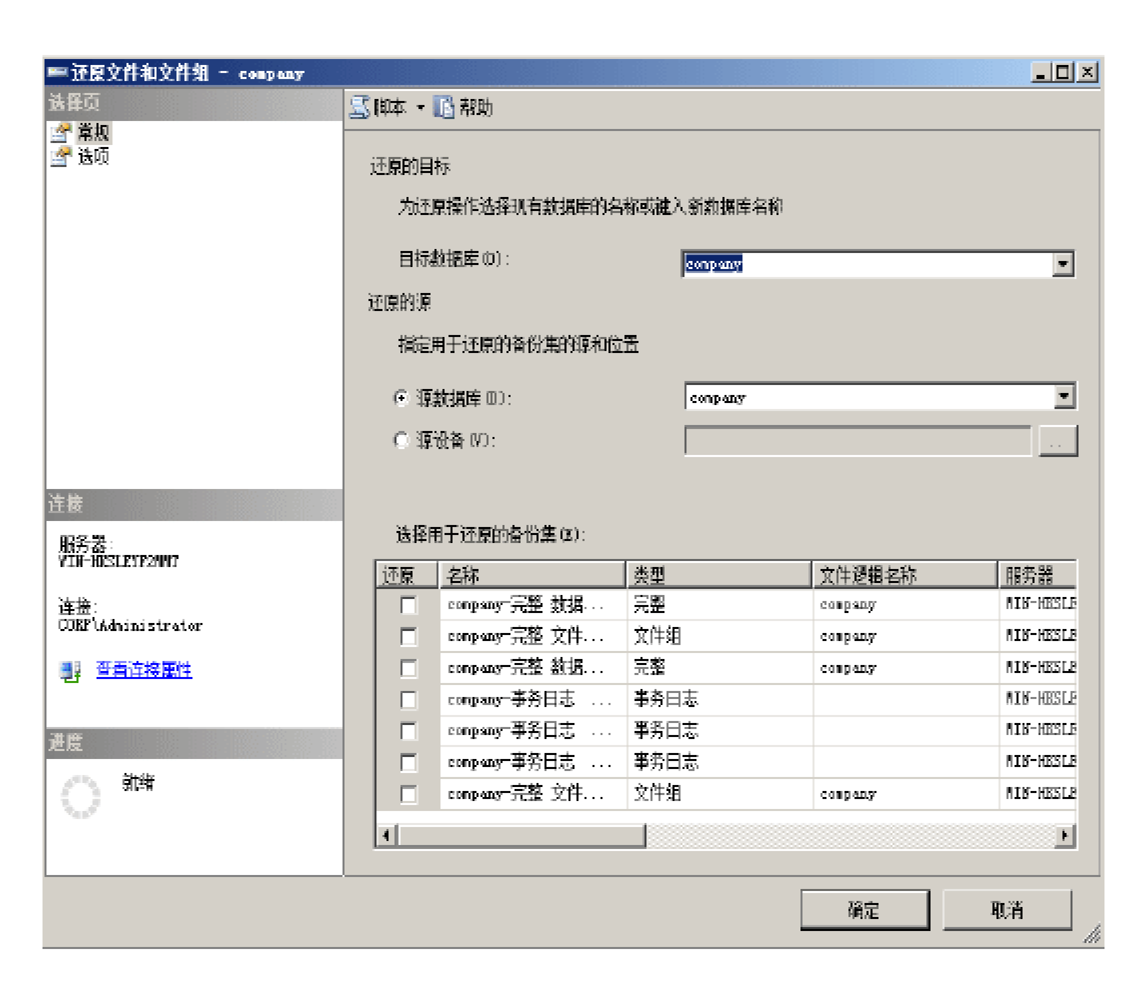


图 17.32 “还原文件和文件组 - company”对话框



02 选择“源设备”单选按钮，单击“…”按钮，显示“指定备份”对话框。在“备份媒体”下拉列表中选中“备份设备”选项，单击“添加”按钮，显示如图 17.33 所示“选择备份设备”对话框，在“备份设备”下拉列表框中，选择“company”选项。

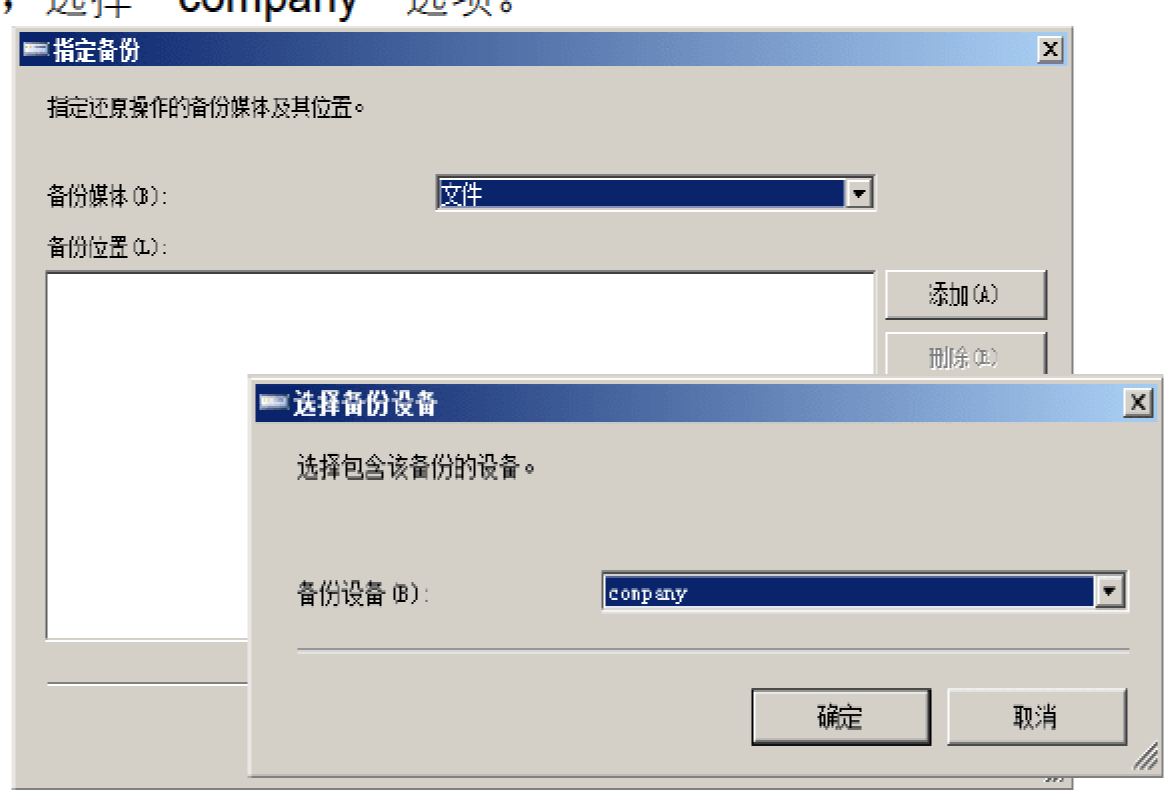


图 17.33　选择备份设备

03 连续单击“确定”按钮，返回“还原文件和文件组 - company”对话框，在“选择用户还原的备份集”文本框中，选中需要恢复的文件组，单击“确定”按钮开始还原，还原成功后显示如图 17.34 所示“还原成功”对话框，单击“确定”按钮即可。



图 17.34　“还原成功”对话框

17.3.5　镜像备份

镜像备份是独立文件（数据文件、归档日志、控制文件）的备份。类似于操作系统级的文件备份。镜像备份不是备份集或备份片，也没有被压缩。

01 在“Microsoft SQL Server Management Studio”窗口中，单击“新建查询”按钮。在左上角下拉列表框中，选择需要进行镜像备份的数据库，在右侧窗口中输入以下代码：

```
BACKUP DATABASE Test
TO DISK='d:\company.bak'
MIRROR TO DISK='d:\company1.bak'
WITH FORMAT
```

02 单击“执行”按钮，显示如图 17.35 所示运行结果。



02 选择“源设备”单选按钮，单击“...”按钮，显示“指定备份”对话框。在“备份媒体”下拉列表中选中“备份设备”选项，单击“添加”按钮，显示如图 17.33 所示“选择备份设备”对话框，在“备份设备”下拉列表框中，选择“company”选项。

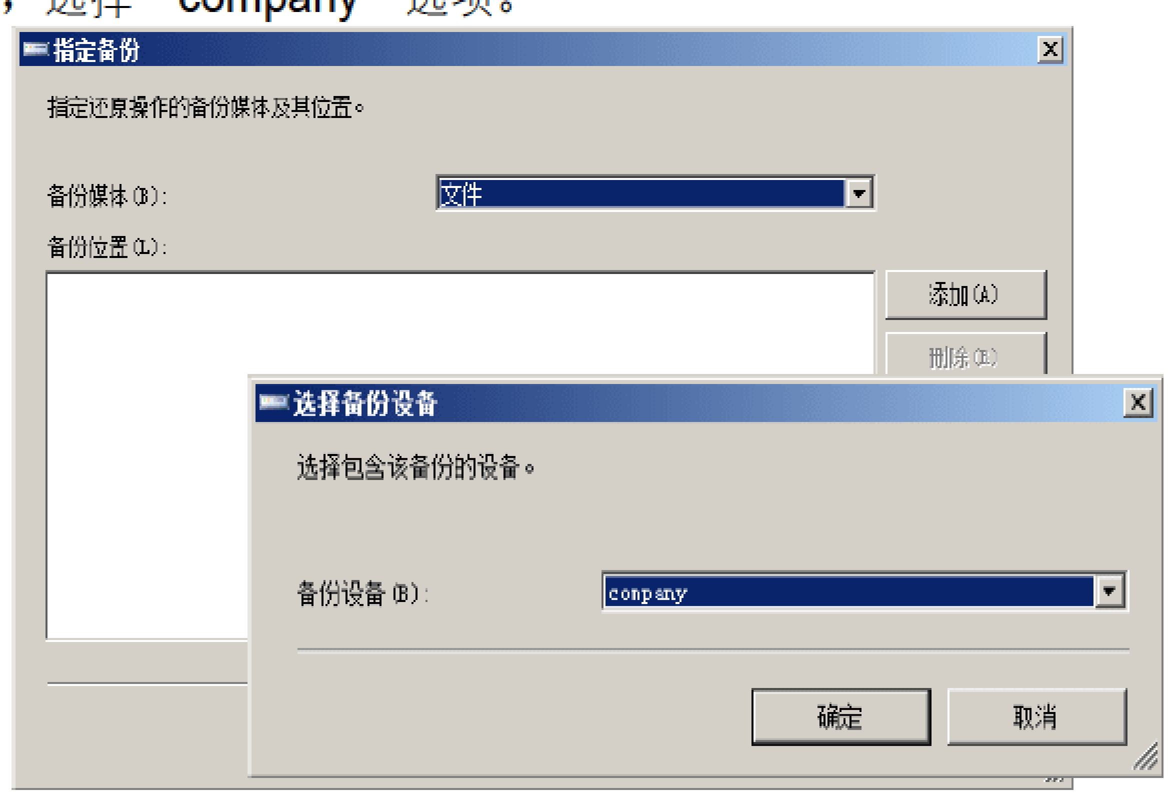


图 17.33　选择备份设备

03 连续单击“确定”按钮，返回“还原文件和文件组 - company”对话框，在“选择用户还原的备份集”文本框中，选中需要恢复的文件组，单击“确定”按钮开始还原，还原成功后显示如图 17.34 所示“还原成功”对话框，单击“确定”按钮即可。



图 17.34　“还原成功”对话框

17.3.5　镜像备份

镜像备份是独立文件（数据文件、归档日志、控制文件）的备份。类似于操作系统级的文件备份。镜像备份不是备份集或备份片，也没有被压缩。

01 在“Microsoft SQL Server Management Studio”窗口中，单击“新建查询”按钮。在左上角下拉列表框中，选择需要进行镜像备份的数据库，在右侧窗口中输入以下代码：

```
BACKUP DATABASE Test
TO DISK='d:\company.bak'
MIRROR TO DISK='d:\company1.bak'
WITH FORMAT
```

02 单击“执行”按钮，显示如图 17.35 所示运行结果。



02 选择“源设备”单选按钮，单击“...”按钮，显示“指定备份”对话框。在“备份媒体”下拉列表中选中“备份设备”选项，单击“添加”按钮，显示如图 17.33 所示“选择备份设备”对话框，在“备份设备”下拉列表框中，选择“company”选项。

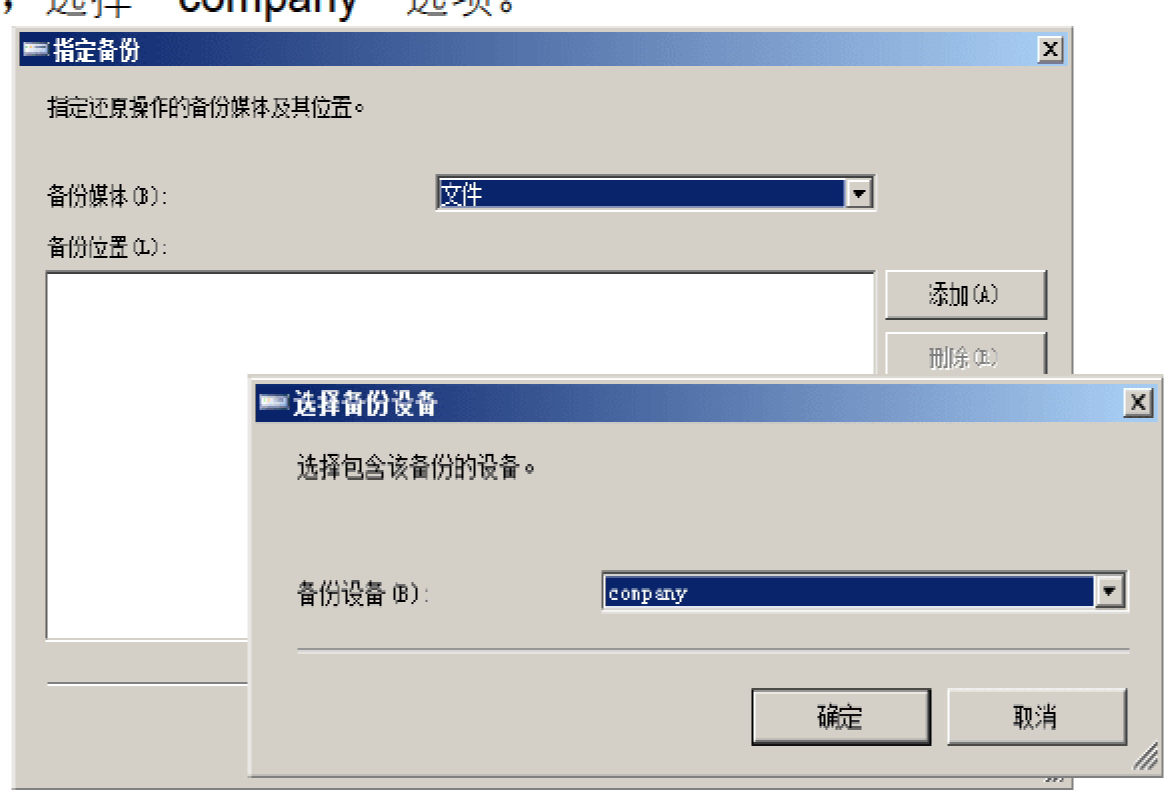


图 17.33　选择备份设备

03 连续单击“确定”按钮，返回“还原文件和文件组 - company”对话框，在“选择用户还原的备份集”文本框中，选中需要恢复的文件组，单击“确定”按钮开始还原，还原成功后显示如图 17.34 所示“还原成功”对话框，单击“确定”按钮即可。



图 17.34　“还原成功”对话框

17.3.5　镜像备份

镜像备份是独立文件（数据文件、归档日志、控制文件）的备份。类似于操作系统级的文件备份。镜像备份不是备份集或备份片，也没有被压缩。

01 在“Microsoft SQL Server Management Studio”窗口中，单击“新建查询”按钮。在左上角下拉列表框中，选择需要进行镜像备份的数据库，在右侧窗口中输入以下代码：

```
BACKUP DATABASE Test
TO DISK='d:\company.bak'
MIRROR TO DISK='d:\company1.bak'
WITH FORMAT
```

02 单击“执行”按钮，显示如图 17.35 所示运行结果。



02 选择“源设备”单选按钮，单击“...”按钮，显示“指定备份”对话框。在“备份媒体”下拉列表中选中“备份设备”选项，单击“添加”按钮，显示如图 17.33 所示“选择备份设备”对话框，在“备份设备”下拉列表框中，选择“company”选项。

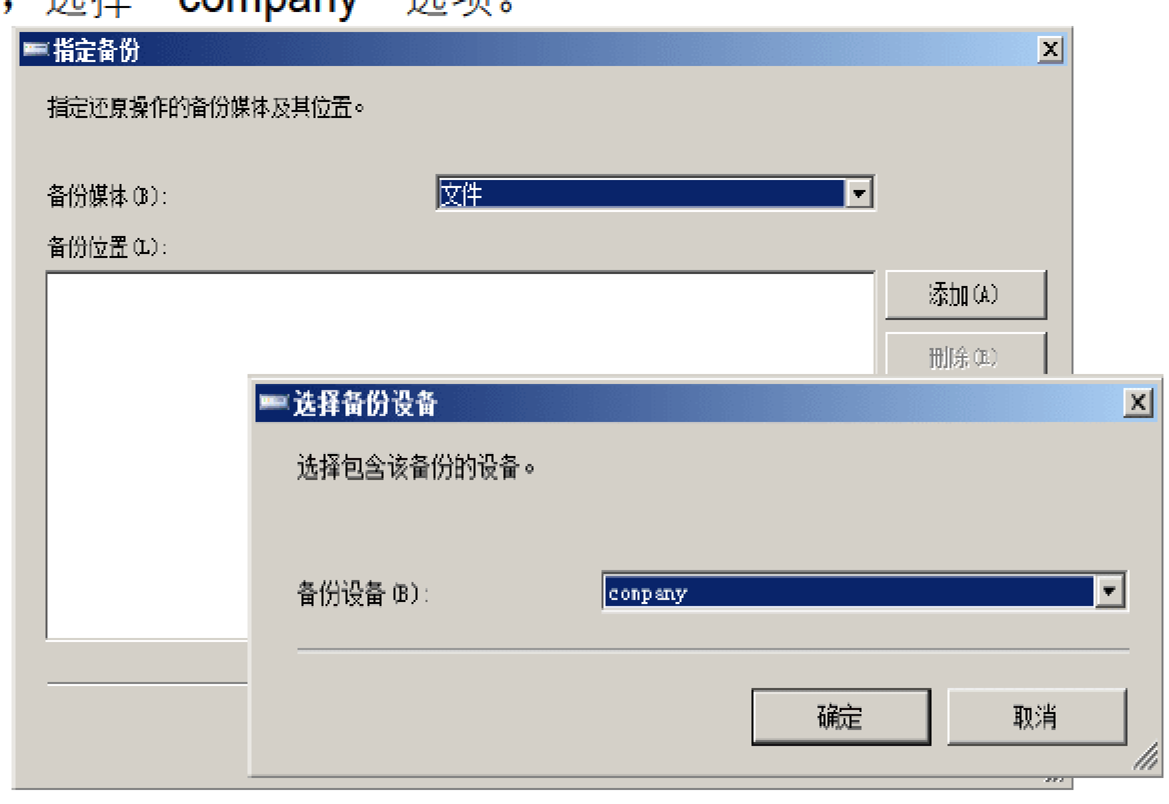


图 17.33　选择备份设备

03 连续单击“确定”按钮，返回“还原文件和文件组 - company”对话框，在“选择用户还原的备份集”文本框中，选中需要恢复的文件组，单击“确定”按钮开始还原，还原成功后显示如图 17.34 所示“还原成功”对话框，单击“确定”按钮即可。



图 17.34　“还原成功”对话框

17.3.5　镜像备份

镜像备份是独立文件（数据文件、归档日志、控制文件）的备份。类似于操作系统级的文件备份。镜像备份不是备份集或备份片，也没有被压缩。

01 在“Microsoft SQL Server Management Studio”窗口中，单击“新建查询”按钮。在左上角下拉列表框中，选择需要进行镜像备份的数据库，在右侧窗口中输入以下代码：

```
BACKUP DATABASE Test
TO DISK='d:\company.bak'
MIRROR TO DISK='d:\company1.bak'
WITH FORMAT
```

02 单击“执行”按钮，显示如图 17.35 所示运行结果。



02 选择“源设备”单选按钮，单击“...”按钮，显示“指定备份”对话框。在“备份媒体”下拉列表中选中“备份设备”选项，单击“添加”按钮，显示如图 17.33 所示“选择备份设备”对话框，在“备份设备”下拉列表框中，选择“company”选项。

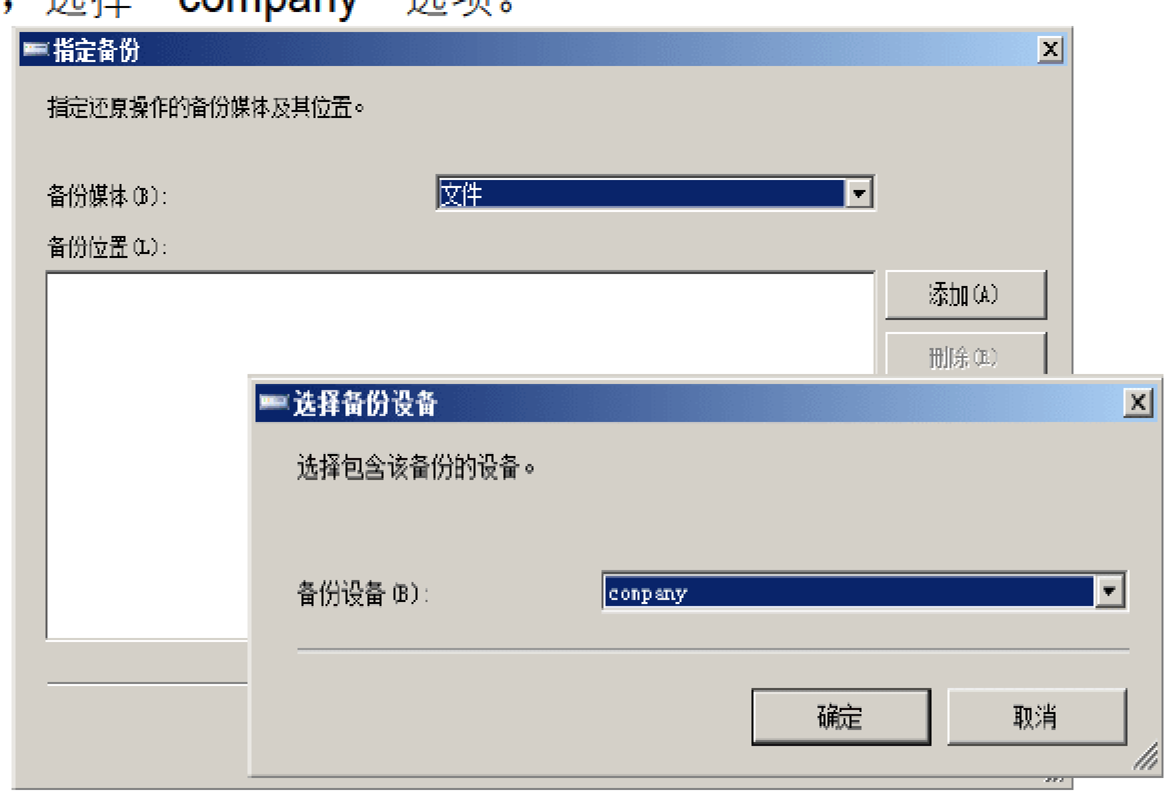


图 17.33　选择备份设备

03 连续单击“确定”按钮，返回“还原文件和文件组 - company”对话框，在“选择用户还原的备份集”文本框中，选中需要恢复的文件组，单击“确定”按钮开始还原，还原成功后显示如图 17.34 所示“还原成功”对话框，单击“确定”按钮即可。



图 17.34　“还原成功”对话框

17.3.5　镜像备份

镜像备份是独立文件（数据文件、归档日志、控制文件）的备份。类似于操作系统级的文件备份。镜像备份不是备份集或备份片，也没有被压缩。

01 在“Microsoft SQL Server Management Studio”窗口中，单击“新建查询”按钮。在左上角下拉列表框中，选择需要进行镜像备份的数据库，在右侧窗口中输入以下代码：

```
BACKUP DATABASE Test
TO DISK='d:\company.bak'
MIRROR TO DISK='d:\company1.bak'
WITH FORMAT
```

02 单击“执行”按钮，显示如图 17.35 所示运行结果。



02 选择“源设备”单选按钮，单击“...”按钮，显示“指定备份”对话框。在“备份媒体”下拉列表中选中“备份设备”选项，单击“添加”按钮，显示如图 17.33 所示“选择备份设备”对话框，在“备份设备”下拉列表框中，选择“company”选项。

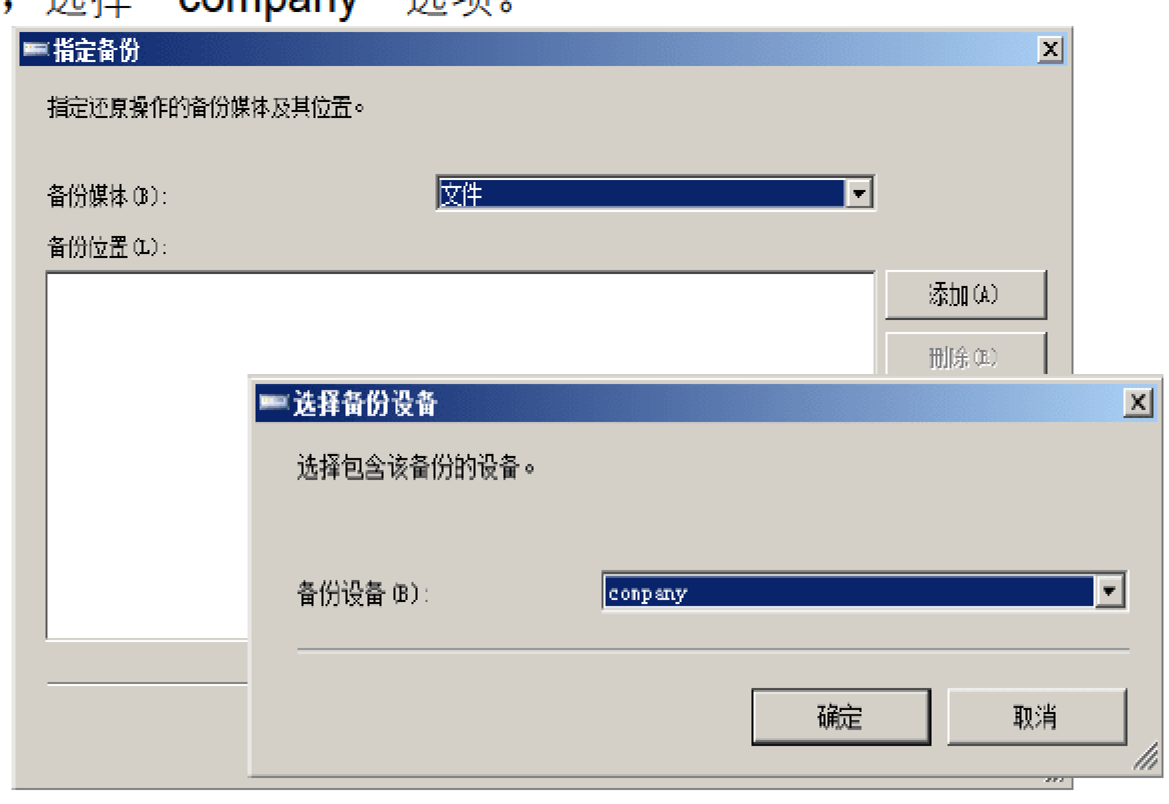


图 17.33　选择备份设备

03 连续单击“确定”按钮，返回“还原文件和文件组 - company”对话框，在“选择用户还原的备份集”文本框中，选中需要恢复的文件组，单击“确定”按钮开始还原，还原成功后显示如图 17.34 所示“还原成功”对话框，单击“确定”按钮即可。



图 17.34　“还原成功”对话框

17.3.5　镜像备份

镜像备份是独立文件（数据文件、归档日志、控制文件）的备份。类似于操作系统级的文件备份。镜像备份不是备份集或备份片，也没有被压缩。

01 在“Microsoft SQL Server Management Studio”窗口中，单击“新建查询”按钮。在左上角下拉列表框中，选择需要进行镜像备份的数据库，在右侧窗口中输入以下代码：

```
BACKUP DATABASE Test
TO DISK='d:\company.bak'
MIRROR TO DISK='d:\company1.bak'
WITH FORMAT
```

02 单击“执行”按钮，显示如图 17.35 所示运行结果。

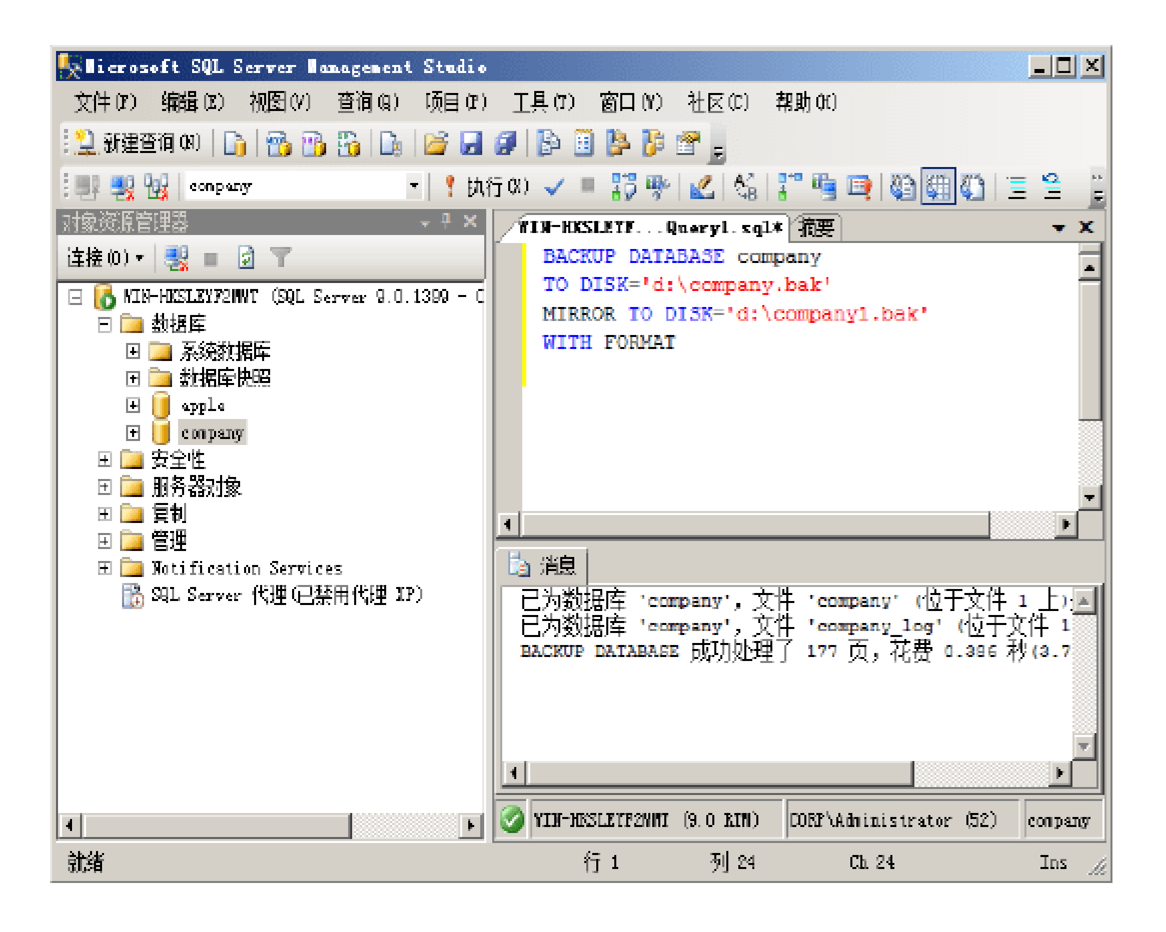


图 17.35 “Microsoft SQL Server Management Studio”窗口

17.3.6 密码备份

Microsoft SQL Server 2005 支持密码验证功能，管理员在备份时设置密码，当恢复时需要使用该密码才能正常恢复，否则即使其他人得到数据库的备份文件也无法还原该数据库。

01 在“Microsoft SQL Server Management Studio”窗口中，单击“新建查询”按钮。在左上角下拉列表中选择需加密的数据库（以 master 为例），在右侧窗口中输入以下代码：

```
BACKUP DATABASE company
TO DISK='d:\company.bak'
with password='123'
```

02 单击“执行”按钮，显示如图 17.36 所示运行结果。此时打开 D 盘即可看到已备份文件。

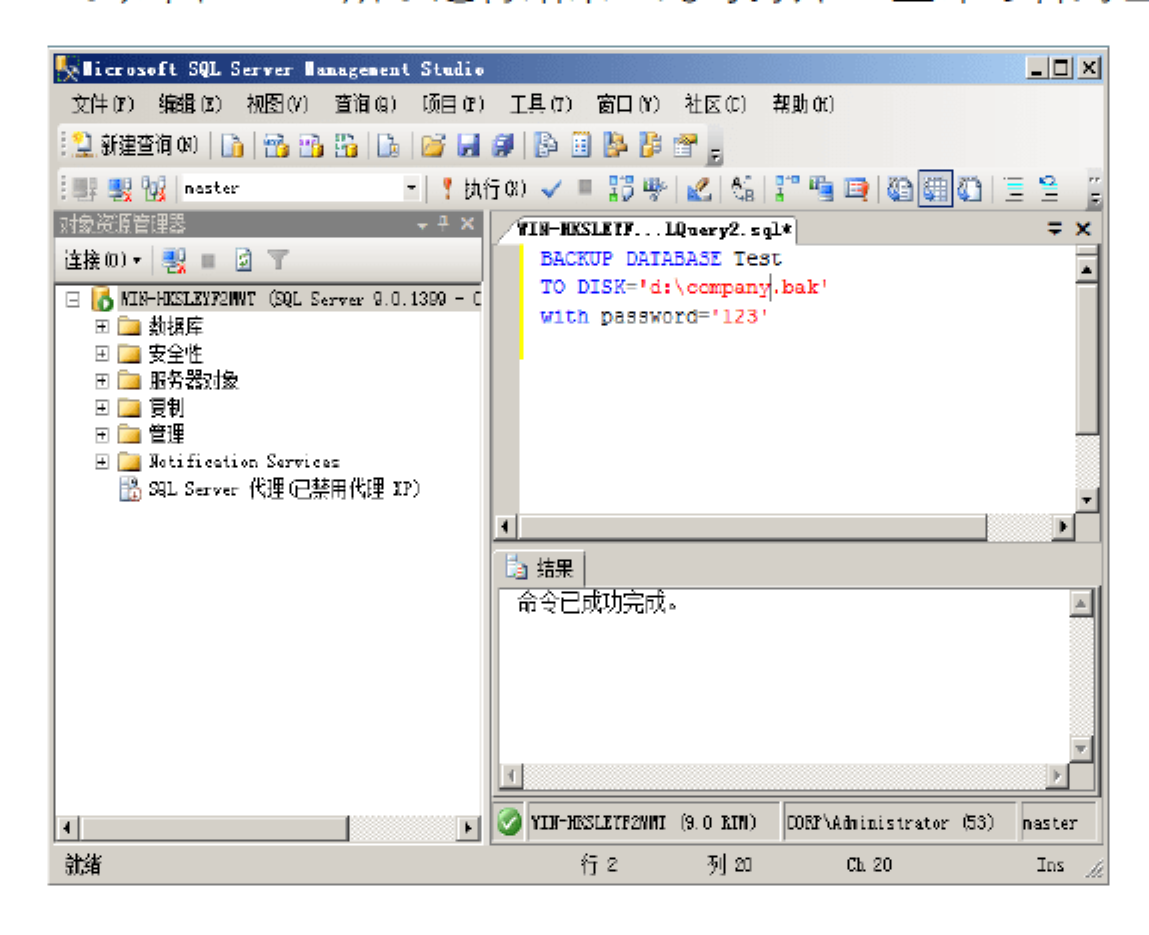


图 17.36 “Microsoft SQL Server Management Studio”窗口



17.3.7　用快照恢复数据库

数据库快照可以为数据库创建一个在某个时间点上的只读副本，适合对实时性要求不高的应用，例如工资报表、数据查询等，如果数据库出现错误，可以将数据库恢复到创建快照时的状态。

1. 创建快照

根据源数据库的当前大小，确保有足够的磁盘空间存放数据库快照。数据库快照的最大大小为创建快照时源数据库的大小。

01 在“Microsoft SQL Server Management Studio”窗口中，单击“新建查询”选项。在左上角下拉列表中选择需加密的数据库（以 company 为例），在右侧窗口中输入以下代码：

```
CREATE DATABASE newcompany  ON
( NAME = company, FILENAME = 'd:\newcompany.mdf' )
AS SNAPSHOT OF company;
GO
```

02 单击“执行”按钮，显示如图 17.37 所示运行结果。

03 依次选择“WIN-HKSLEYF2MMT”→“数据库”，右击“数据库快照”并在快捷菜单中选择“刷新”选项，如图 17.38 所示。

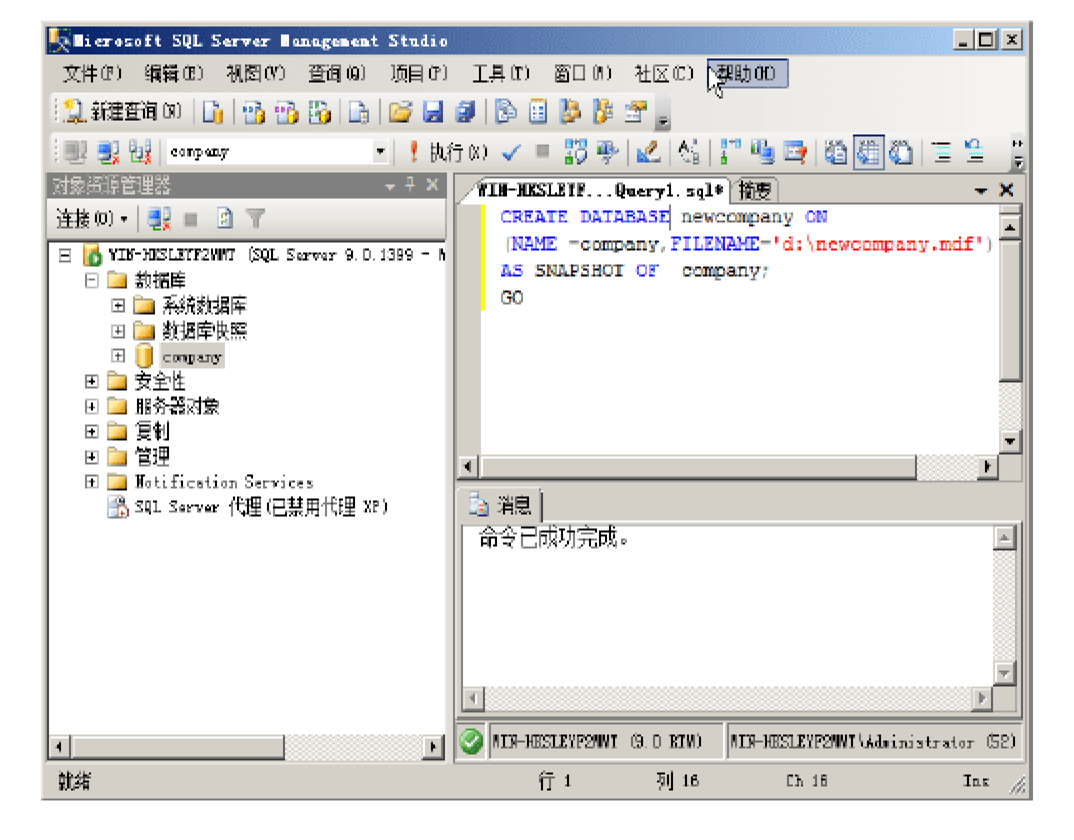


图 17.37　命令运行结果

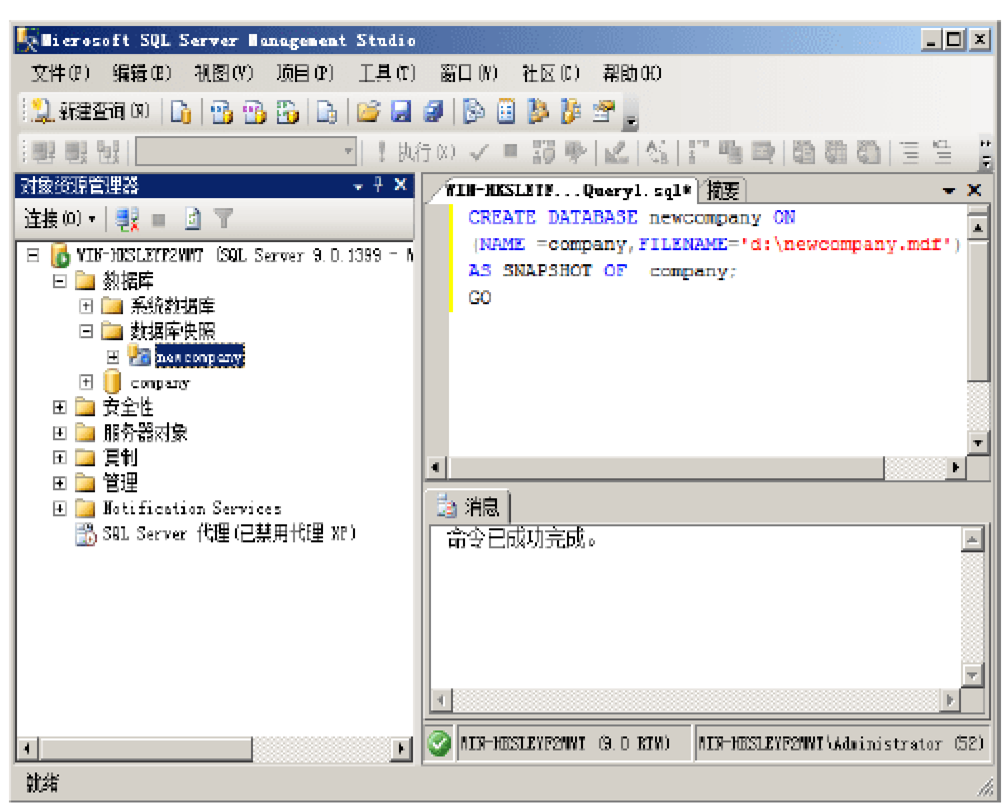


图 17.38　刷新结果

2. 恢复快照

数据库快照不是冗余存储，因此不针对磁盘错误或其他类型的损坏提供任何保护功能，但是如果在联机数据库中发生用户错误，可以将数据库恢复到发生错误之前的数据库快照。

01 在“Microsoft SQL Server Management Studio”窗口中，单击“新建查询”选项。在左上角下拉列表中选择需加密的数据库（以 master 为例），在右侧窗口中输入以下代码:

```
USE company;
RESTORE DATABASE company from
DATABASE SNAPSHOT='newcompany';
GO
```

02 单击“执行”按钮，显示如图 17.39 所示运行结果。

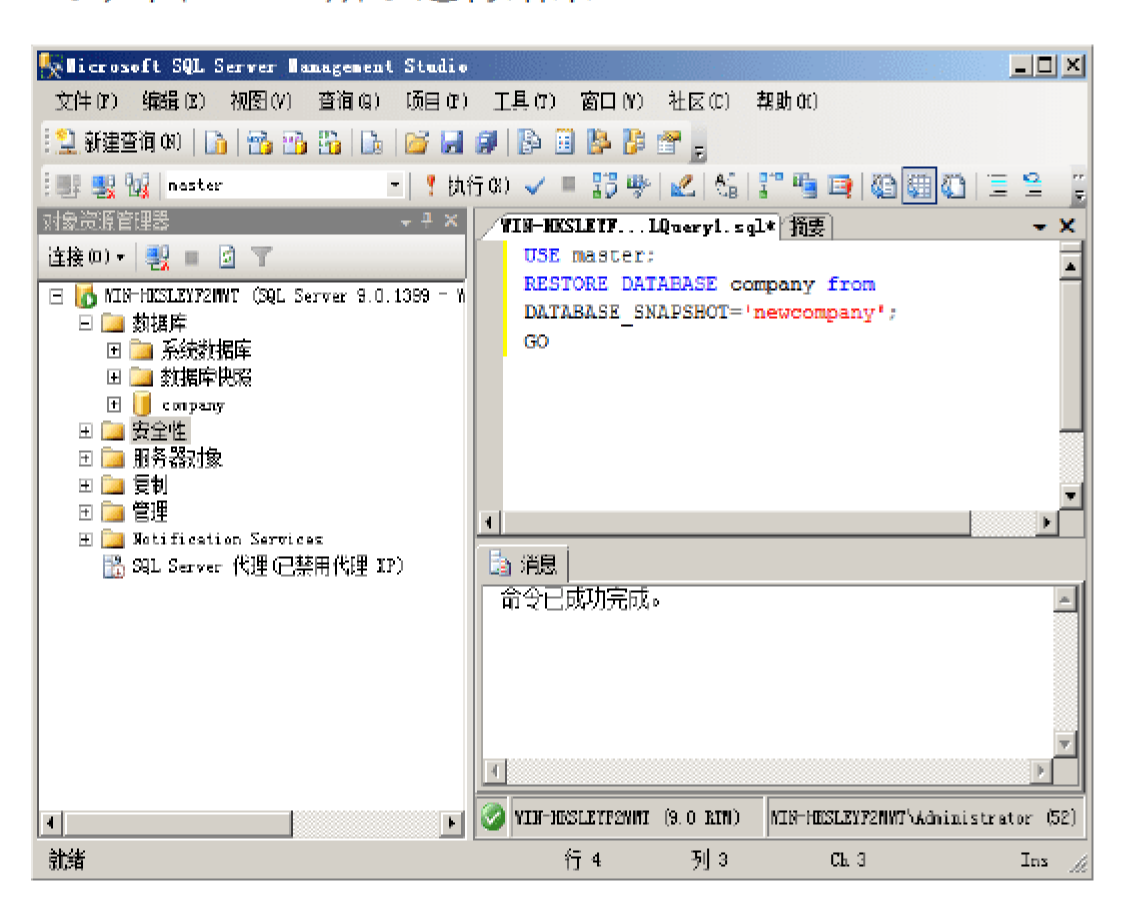


图 17.39　代码代码执行结果

17.4　系统补丁

入侵者通常通过操作系统上的漏洞来进入数据库中，盗取有关信息，所以在安装完 Windows Server 2008 和 Microsoft SQL Server 2005 后应当及时更新补丁程序，避免因系统漏洞而带来的安全威胁。

17.4.1　操作系统补丁

Windows 操作系统是一个非常复杂的软件系统，难免会存在许多的程序漏洞，这些漏洞会被病毒、木马、恶意脚本以及黑客利用，从而影响计算机的使用、网络的安全以及运行的畅通。因此微软公司会不断发布升级程序供用户安装。这些升级程序就是“系统补丁”，因此及时为 Windows 安装系统补丁是十分必要的。

01 在浏览器地址栏中输入 Windows Server 2008 服务器操作系统最新补丁下载地址 http://technet.microsoft.com/zh-cn/bb871013.aspx，打开如图 17.40 所示“下载中心-Windows Server”窗口。

02 从“下载中心-Windows Server”窗口中，显示 Windows Server 2008 服务器操作的最新补丁包是 Windows Server 2008 Service Pack 2 Release Candidate 和 Windows Vista Service Pack 2 Release Candidate 所有语言单行版本（KB948465），单击“Windows Server 2008 Service Pack 2 Release Candidate 和 Windows Vista Service Pack 2 Release Candidate 所有语言单行版本（KB948465）”链接，打开如图 17.41 所示“下载详细信息”窗口。





图 17.40　“下载中心-Windows Server”窗口



图 17.41　“下载详细信息”窗口

03 单击“下载”按钮，即可开始下载，下载完成后，使用默认设置进行安装即可。

17.4.2　数据库补丁

随着最近绝密数据防线屡被突破的消息，人们的目光都聚集在了数据库安全方面。数据库以持续增长的速度遭受到黑客的直接攻击，因此数据库补丁极其重要。

01 在浏览器中打开 SQL Server 最新补丁程序下载地址 http://technet.microsoft.com/zh-cn/bb871006.aspx。Microsoft SQL Server 2005 的最新补丁包为“Service Package3”，单击“SQL Server 2005 SP3”超级链接，打开如图 17.42 所示“下载详细信息”窗口。



图 17.42　“下载详细信息”窗口

02 在“下载详细信息”窗口中，选择 X86 架构的补丁包，点击“下载”按钮即可开始下载，下载完后，使用默认设置进行安装即可。

小　　结

SQL Server 2005 是一个全面的数据平台，使用集成的商业智能工具提供了企业级的数据管理，为关系型数据和结构化数据提供了更安全可靠的存储功能。通过对传输数据的加密，数据库访问权限的安全控制、补丁的更新，保证数据库安全，为了防止数据库遭到不可逆转的破坏，管理员应当对数据做好安全备份工作。

习　　题

1. 常用的数据库有哪些，各有什么优点？
2. 使用 MSBA 可以扫描哪些方面的漏洞？
3. 如果数据库遭到破坏应如何还原数据？
4. 通过哪些手段可以加强数据库服务器的安全性？

实验：禁止对数据库的写入和修改

实验目的

掌握保护数据库安全的基本方法。

实验内容

禁止对数据库的写入和修改，保证非法入侵者利用数据库脚本完成对数据的修改，从而保证数据库的安全。

实验步骤

1. 打开数据库属性。
2. 设置数据库为只读。
3. 完成对只读数据库的安全配置。

第18章

Windows Server 2008 系统安全新技术

系统安全性问题一直是倍受用户关注的问题，也是微软公司产品的研发方向。Windows Server 2008 网络操作系统，不仅凝聚了微软多年以来的成熟技术，而且新增了许多实用功能。无论是系统安全性，还是网络服务的功能性，都有了质的飞跃。本章主要对 Windows Server 2008 系统安全方面的新特性和新技术加以介绍。

本章导读

- 系统新增安全功能
- 升级的安全特性
- 应用服务器角色安全新特性

18.1 系统新增安全功能

相对于先前的 Windows Server 2003 和 Windows 2000 Server 系统，Windows Server 2008 新增了不少安全功能，例如 BitLocker 驱动加密、网络访问保护、用户帐户控制以及高级安全 Windows 防火墙等。

18.1.1 BitLocker 驱动加密

BitLocker 驱动加密是 Windows Server 2008 中一项基于硬件加密的关键新安全功能，用于保护分支办公室中的服务器安全。

1. BitLocker 的实现方式与功能

BitLocker 驱动加密的实现模式有 TPM（受信平台模块）芯片模式和 U 盘模式两种，分别适用于不同的系统环境。

- TPM 芯片模式。要求服务器主板集成 TPM v1.2 芯片，系统会将解锁磁盘所需的根密钥存放在 TPM 芯片里；
- U 盘模式。如果没有 TPM 芯片，但计算机 BIOS 支持开机时访问 U 盘，还可以采用 U 盘模式实现 BitLocker 驱动器加密。可以将解锁磁盘所需的启动密钥存放在 U 盘里，开机时必须插入 U 盘，才能解锁加密的 Windows 卷，访问 Windows 系统。

TPM 模式可以实现最严格的安全保护措施。TPM 模式除了可实现 U 盘模式所支持的全卷加密之外，还支持系统启动部件的完整性检测。另外，在企业淘汰处理服务器时，使用 BitLocker 加密功能可以确保重要数据信息不会外泄。

在设置 BitLocker 加密时，系统会把 MBR（主引导记录）、NTFS 卷的引导扇区、NTFS 引导代码、BitLocker 密钥等启动部件做一个“快照”，保存在 TPM 芯片里。每次系统启动时，会自动与 TPM 芯片里保存的快照进行比较，只有发现这些启动部件没有发生变化，才会继续解密过程。很显然，USB 模式的 BitLocker 加密，无法实现启动部件的完整性检测。

BitLocker 驱动器加密可以提供如下功能：

- 系统脱机时的数据保护。加密整个 Windows 卷，包括用户数据和系统文件、休眠文件、换页文件和临时文件；为第三方应用程序提供伞式保护；第三方应用程序安装在加密卷上时会自动受益；
- 确保引导过程的完整性。因为它可以提供一种方法来检查是否保持了早期引导文件的完整性，并且这些文件未被恶意修改（例如通过引导区病毒修改）；



- 防止系统受到脱机情况下基于软件的攻击。任何可以引导系统的替代软件，都无法访问保护此 Windows 卷的根密钥；
- 当被篡改时锁定系统。如果任何监控文件被篡改，则系统将不启动。由于系统无法正常启动，这会警告用户发生了篡改情况；
- 通过用以下方式简化设备的重复利用：缩短以安全方式永久删除驱动器上所有数据的时间；仅通过删除访问驱动器所需的密钥，就可以使加密卷上的数据变为无用数据。

要使用 BitLocker 驱动器加密，计算机必须满足由 BitLocker Windows Server 2008 系统徽标要求指定的要求，主要包括如下内容：

- 系统必须具备 TPM v1.2 芯片；
- TPM 可对系统引导过程完整性进行测量和报告；
- 系统必须具备符合 TCG v1.2（受信计算组，Trusted Computing Group）的 BIOS1；
- BIOS 可为操作系统引导建立信任链；
- 系统必须包括对 TCG 指定的“静态根可信度测量”（SRTM）的支持；
- 系统 BIOS 必须支持 U 盘启动，包括引导操作系统时在 U 盘上读写数据；
- 计算机上至少具备两个要运行的卷。“操作系统卷”（或引导卷）是包含 Windows 操作系统及其支持文件的卷，它必须使用 NTFS 来格式化。此卷上的数据由 BitLocker 保护；“系统卷”是在 BIOS 引导平台后加载 Windows 计算机时所需的特定硬件文件所在的卷。为使 BitLocker 正常工作，系统卷不得加密，必须有别于操作系统卷，并且必须使用 NTFS 进行格式化。系统卷的可用空间至少为 1.5 GB。写入此卷的数据（包括附加的用户数据）不受 BitLocker 保护。

2. BitLocker 在服务器上的应用

部署多种安全防御措施的中心机房可以确保服务器的物理安全，但是对于分支机构中的服务器而言，物理安全防护是非常脆弱的。在此类服务器上启用 BitLocker 功能后即可对操作系统卷加密，还可以针对 IT 管理员希望用 WMI 保护的任何数据卷来通过 WMI 启用。BitLocker 驱动器加密为服务器提供的安全防护功能如下：

- PIN 支持。对于将重启动速度视为一种因素或在重启动时无法实现人为干预的服务器，建议不要启用 PIN 功能。在许多服务器环境中，正常运行时间和远程管理至关重要；
- 启动密钥支持。对服务器支持 USB 启动密钥，确保系统只有在 USB 启动密钥的支持下才能启动。需要注意的是，每次重新启动服务器时都需要人为干预才能实现最佳的数据保护。另外，保存启动密钥的 U 盘也要妥善保管，避免使用后遗留在服务器上；
- 密钥链。保护服务器数据卷的密钥独立于保护操作系统卷的密钥。要使系统自动安装这些卷，还要将保护数据卷的密钥链在加密状态下存储在当前引导的卷上。特别是，在当前引导卷的注册表中有一个外部包装密钥（EWK），它是一个 256 位的 AES 密钥，用于保护数据卷的 VMK（卷主密钥，Volume Master Key）。由于 EWK 存储在加密的操作系统卷中，因此它受 BitLocker 以及 Windows Server 2008 系统自身的保护。如果操作系

统进入恢复模式，则数据卷将一直受到保护，直到操作系统退出恢复模式为止；

- 自动解锁。自动解锁功能满足的是在引导期间对数据卷自动解锁而不需要人为干预的需要。启用自动解锁时可将数据卷 EWK 的纯文本副本提交到所引导操作系统的注册表中。在没有成功访问加密操作系统卷的情况下，无法访问数据卷上的数据。首次尝试从 Windows 读取或查询数据卷会导致其 VMK 被解密（通过从注册表读取 EWK 来实现）。如果在操作系统卷中关闭 BitLocker，则 BitLocker 还会清除操作系统卷注册表中的密钥资料。在这些情况下，用户必须提供密钥才能访问数据卷；
- 群集配置。Windows Server 2008 中的 BitLocker 驱动器加密可以很好地支持群集配置；
- 数据卷的恢复。数据卷的恢复类似于操作系统卷的恢复。在出现故障前（最好在设置时），必须在其他介质上存储 EWK 的副本。如果数据卷损坏、被移动到新平台或操作系统卷无法为自动解锁检索 EWK，则用户可插入含有 EWK 副本的存储介质。

3. BitLocker 安全注意事项

任何安全措施都不可能做到万无一失。同样，BitLocker 也无法为计算机防御所有可能的攻击。如果 USB 启动密钥保留在计算机中，或者 PIN、Windows 登录密码没有保密，则 BitLocker 保护可能也不起作用。

仅 TPM 身份验证模式（即没有启动密钥或 PIN）提供最透明的组织用户体验，而这需要基线级别的数据保护以符合安全策略。仅 TPM 模式最容易部署、管理和使用。这更适合于无人参与的计算机或必须在无人参与时重新启动的计算机。

但是，仅 TPM 模式提供最少量的数据保护。该模式防护某些修改早期启动组件的攻击，但是防护级别受操作系统、硬件或 BIOS 中的潜在安全漏洞的影响。添加 PIN 或 USB 启动密钥可以帮助减少很多此类攻击。如果您组织的几个部门在移动计算机上具有认为非常敏感的数据，则考虑在这些计算机上部署具有多重身份验证的 BitLocker。

4. 安装和应用 BitLocker

（1）为 BitLocker 驱动器加密设置磁盘卷

BitLocker 驱动器加密对服务器磁盘分区的格式有严格要求，因此部署操作系统之前，必须先在希望应用 BitLocker 驱动器加密的计算机上，按照需要设置磁盘卷，然后再安装 Windows Server 2008。

---

01 用 Windows Server 2008 安装光盘引导计算机，显示如图 18.1 所示“安装 Windows”对话框。

02 单击左下方的“修复计算机”链接，显示如图 18.2 所示“系统恢复选项”对话框，由于是全新的硬盘，这里应该是空的，如果硬盘上存在其他 Windows 系统，则将显示在该列表中。





图 18.1　“安装 Windows”对话框

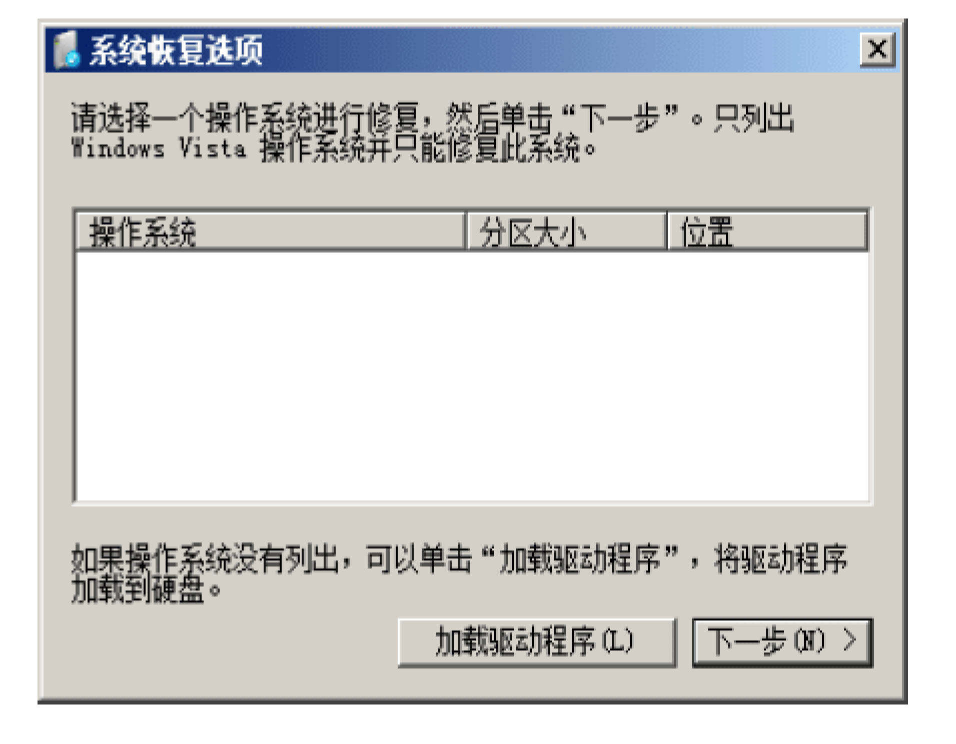


图 18.2　“系统恢复选项”对话框

03 单击“下一步”按钮，显示如图 18.3 所示“选择恢复工具”对话框。

04 单击“命令提示符”链接，打开命令提示符窗口。输入 diskpart 命令并按“Enter”键进入 DISKPART>提示符。

05 在 DISKPART>提示符下，输入 select disk 0 命令并按“Enter”键，以选中该磁盘。

06 输入 clean 命令并按“Enter”键，清空该磁盘上的分区表。

07 输入以下命令： create partition primary size=2000，并按“Enter”键，创建一个 2 GB 的主分区。

08 输入以下命令： assign letter=M，并按回车键，将该分区的盘符设置为 M。

09 输入 active 命令并按“Enter”键，将该分区设置为活动分区。操作结果如图 18.4 所示。

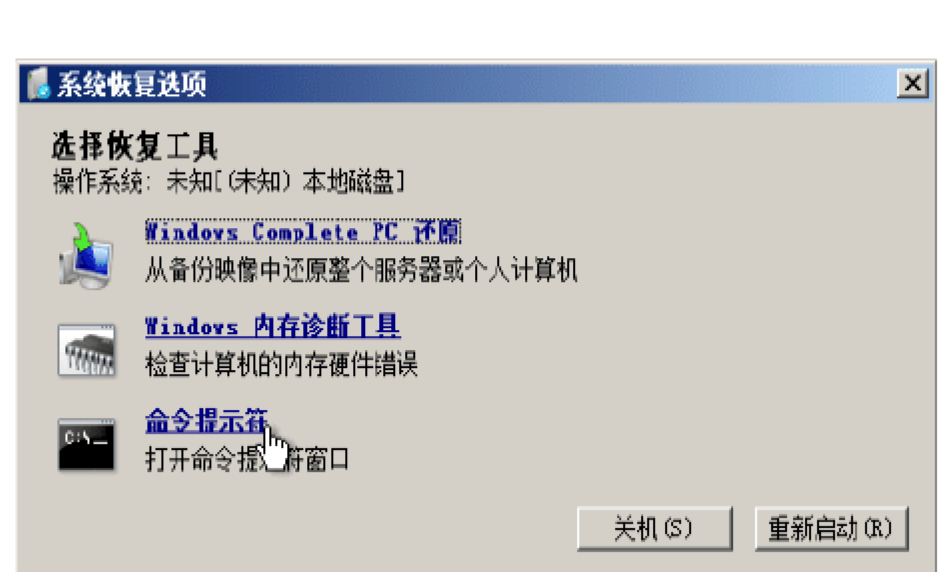


图 18.3　“选择恢复工具”对话框



图 18.4　创建并激活系统卷

10 输入以下命令： create partition primary size=100000，并按“Enter”键，创建 Windows 操作系统分区。

11 输入以下命令：assign letter=C，并按“Enter”键，将该分区的盘符设置为 C。

12 输入以下命令：create partition primary，并按“Enter”键，将剩余磁盘空间作为数据分区。

13 输入以下命令：assign letter=E，并按“Enter”键，将该分区的盘符设置为 E。

14 输入以下命令：list volume，并按“Enter”键，检查新建的所有分区。显示结果如图 18.5 所示。

15 输入以下命令：exit，退出 DISKPART>提示符。

16 在命令提示符下分别输入以下命令并按“Enter”键：

```
format C: /Y /Q /FS:NTFS
format E: /Y /Q /FS:NTFS
```

```
format M: /Y /Q /FS:NTFS
```

把所有主分区格式化为 NTFS 文件系统，如图 18.6 所示。

```
DISKPART> create partition primary size=100000
DiskPart 成功地创建了指定分区。
DISKPART> assign letter=C
DiskPart 成功地分配了驱动器号或装载点。
DISKPART> create partition primary
DiskPart 成功地创建了指定分区。
DISKPART> assign letter=E
DiskPart 成功地分配了驱动器号或装载点。
DISKPART> list volume
  卷 ###      LTR  标签         FS     类型        大小     状态       信息
  ----------  ---  -----------  -----  ----------  -------  ---------  --------
  卷     0     D   KRMSVOL_CN_  UDF    CD-ROM      1955 MB  正常
  卷     1     M                RAW    磁盘分区     2000 MB  正常
  卷     2     C                RAW    磁盘分区       98 GB  正常
* 卷     3     E                RAW    磁盘分区      220 GB  正常
DISKPART>
```

图 18.5　创建 Windows 分区和数据分区

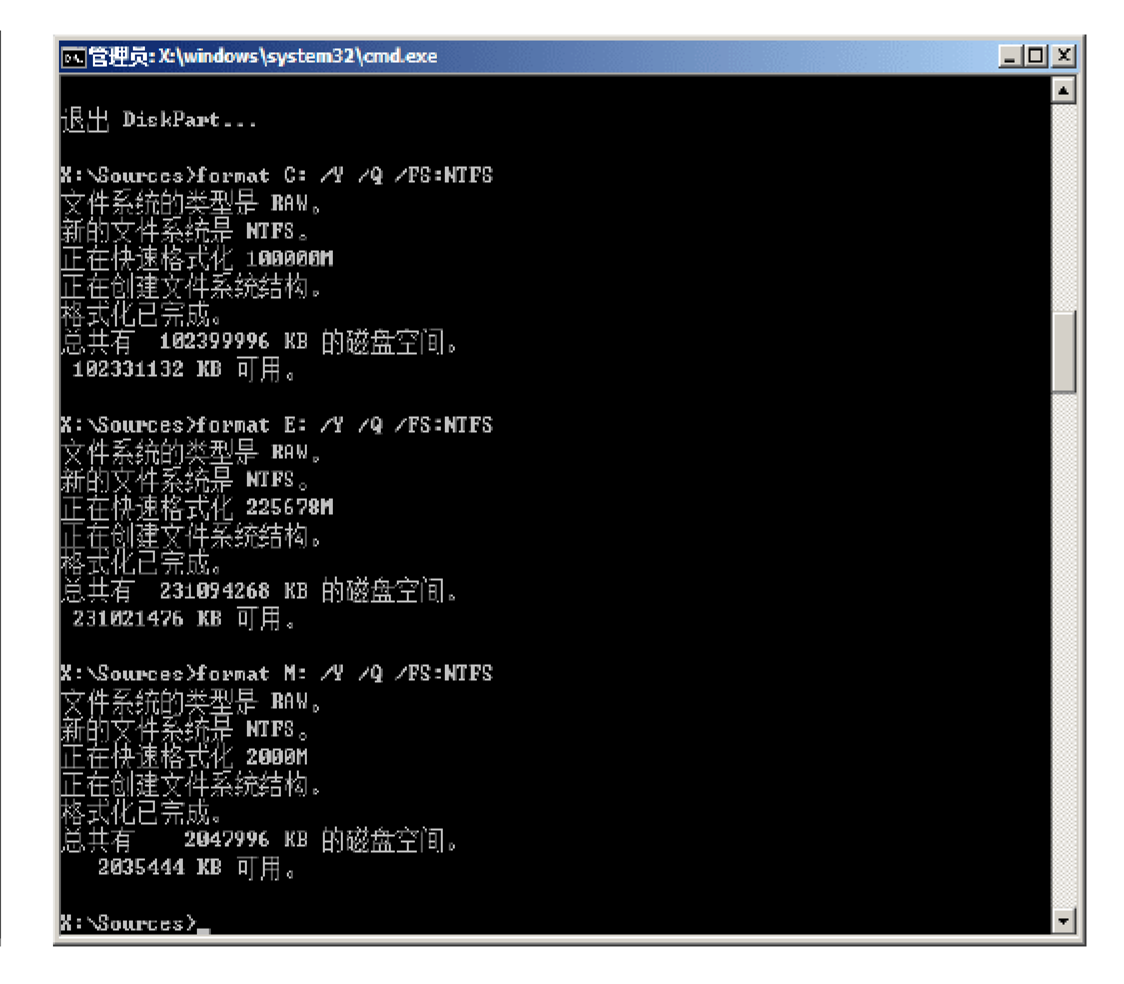


图 18.6　格式化所有分区

17 关闭打开的命令提示符窗口，关闭“系统恢复选项”对话框，回到 Windows Server 2008 系统安装页面，按照常规方式将 Windows Server 2008 安装在先前创建的分区 C:上即可，如图 18.7 所示。

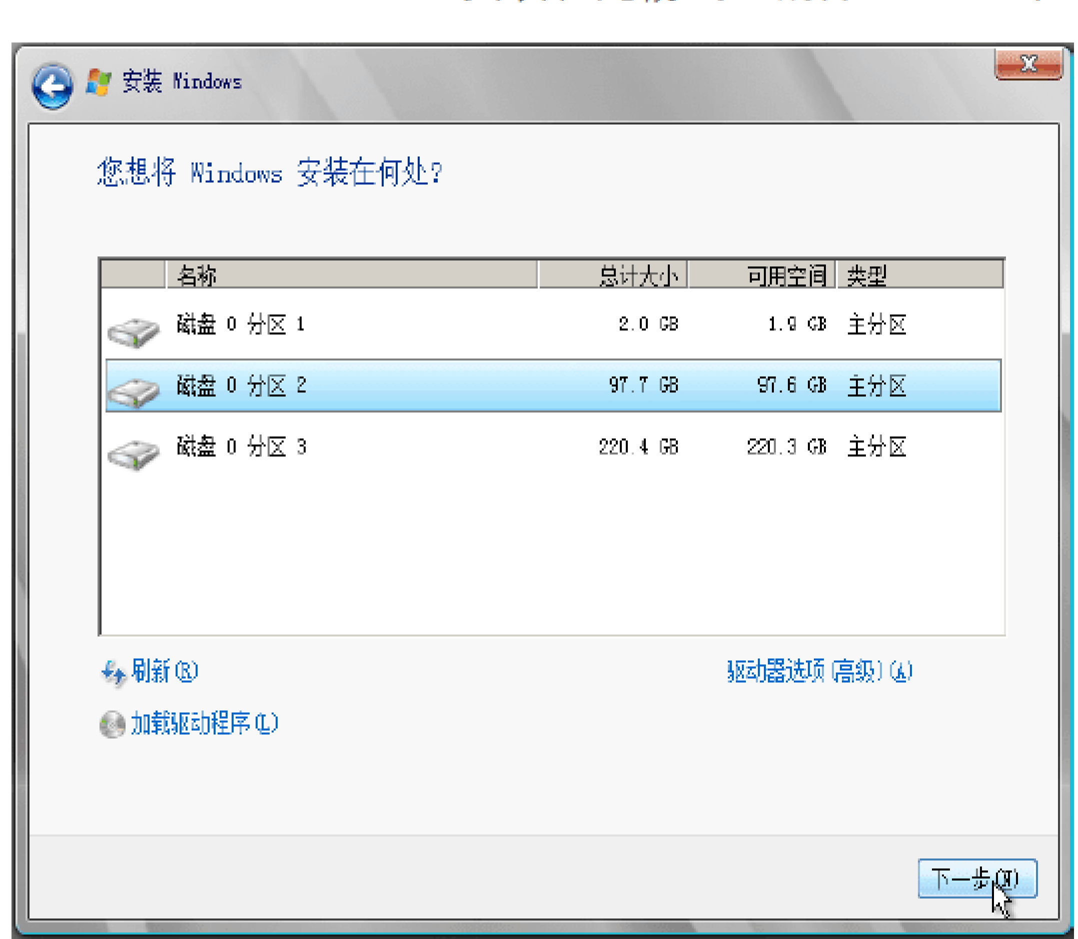


图 18.7　安装 Windows Server 2008

（2）安装 BitLocker

默认情况下，Windows Server 2008 系统中的 BitLocker 驱动器加密功能组件并未随系统自动安装，管理员可以通过“添加功能”的方式安装 BitLocker，如图 18.8 所示。安装 BitLocker 功能后，可根据需要对其进行设置和维护。需要注意的是，在服务器上安装 BitLocker 驱动器加密组件后，必须重新启动计算机。



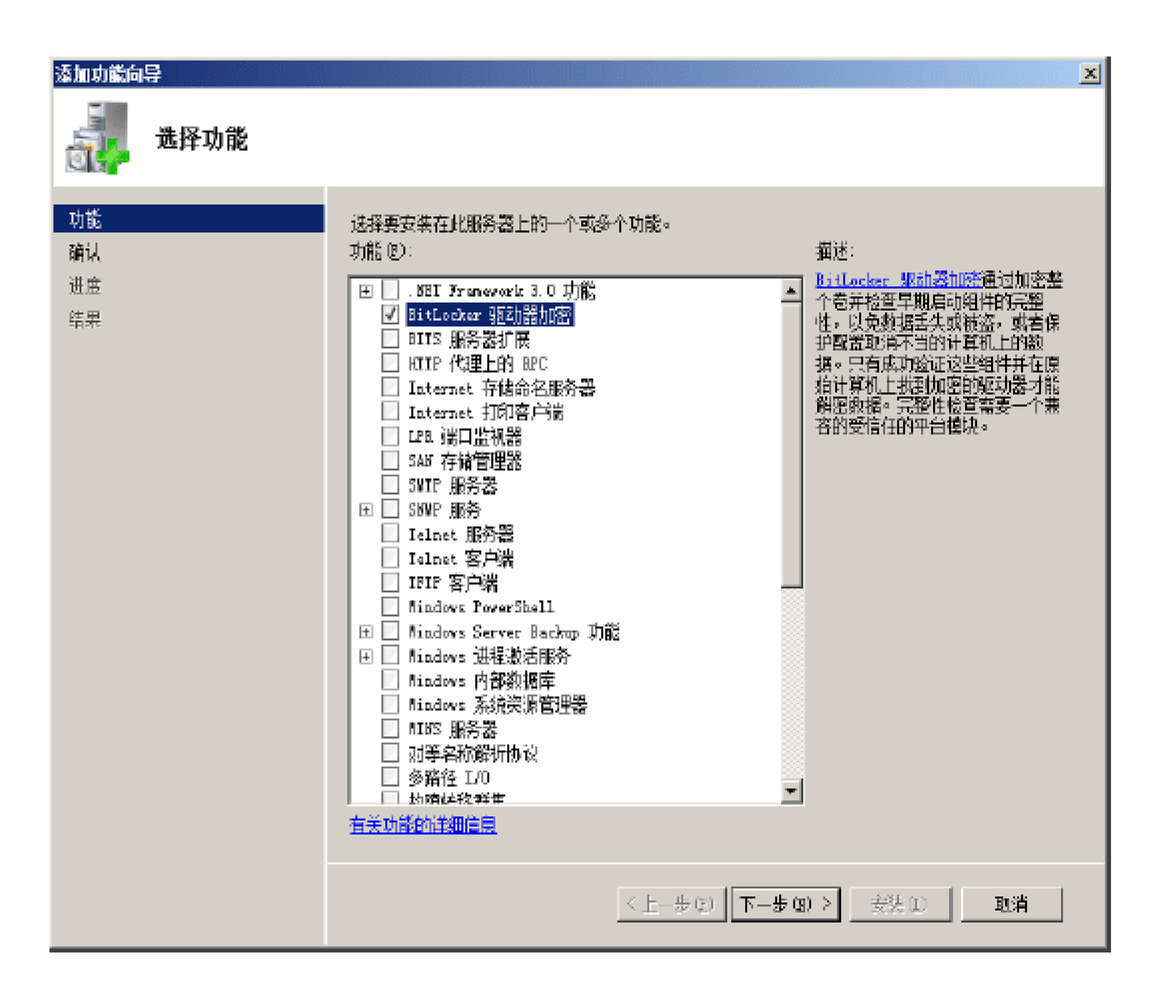


图 18.8　安装 BitLocker 组件

5. 基于 U 盘模式的 BitLocker 加密

并非所有的计算机都已经集成 TPM 芯片，但几乎所有的计算机上都可以使用 U 盘，基于 U 盘模式的 BitLocker 加密方法实现简单，适合于所有用户。需要注意的是，为了确保服务器系统安全，建议准备一个“专项专用”的 U 盘，以免加密信息泄露或感染病毒。

01 单击“开始”按钮，在“开始搜索”文本框中输入“gpedit.msc”并回车，打开“本地组策略编辑器”窗口。依次展开“计算机配置”→“管理模板”→“Windows 组件”→“BitLocker 驱动器加密”节点，如图 18.9 所示。

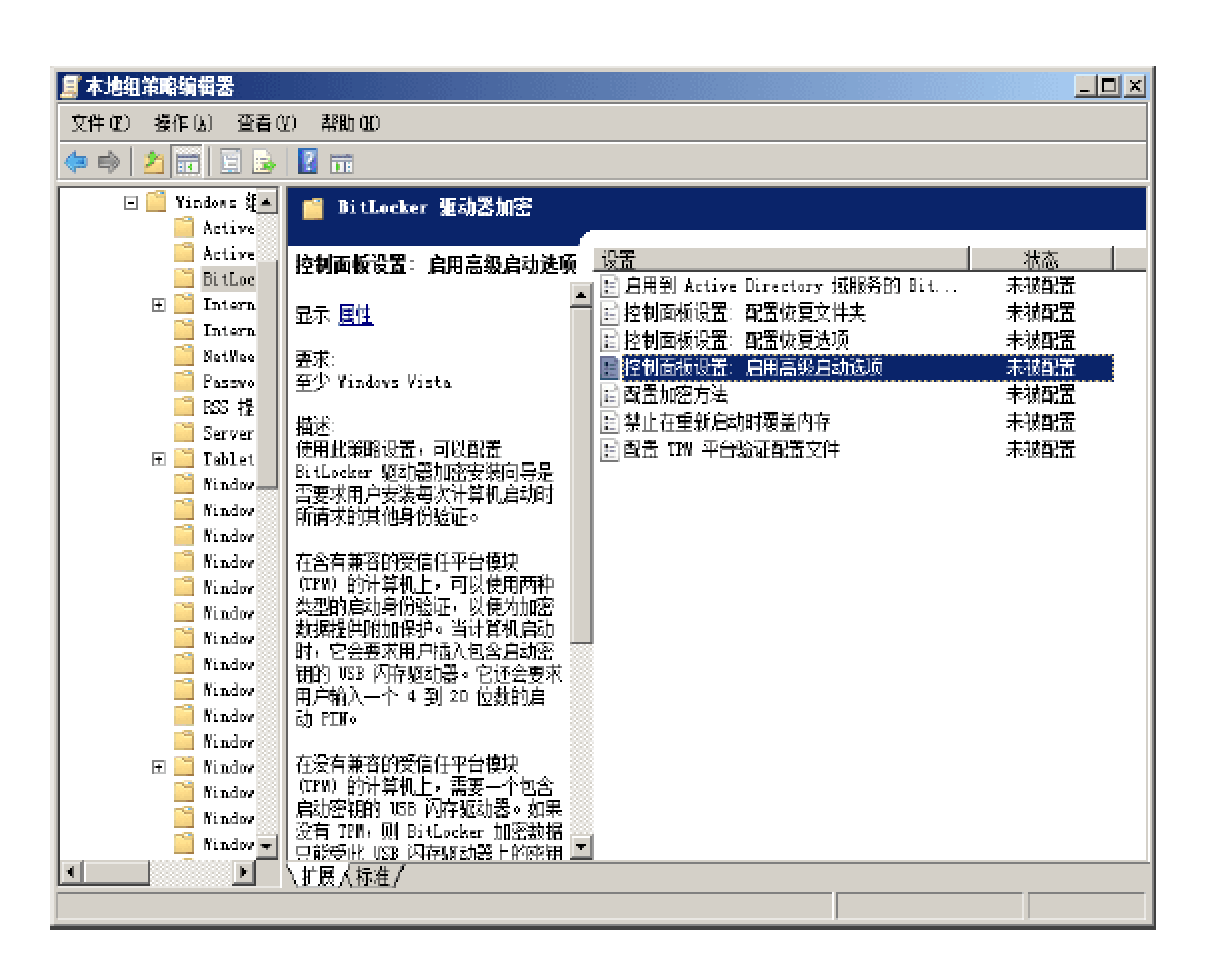


图 18.9　“本地组策略编辑器”窗口

02 双击“控制面板设置 启用高级启动选项”策略，显示如图 18.10 所示“控制面板设置：启用高级启动选项 属性”对话框。首先，选择“已启用”单选按钮，此时“没有兼容的 TPM 时允许 BitLocker”复选框会自动选中，然后，单击“应用”按钮保存设置即可。

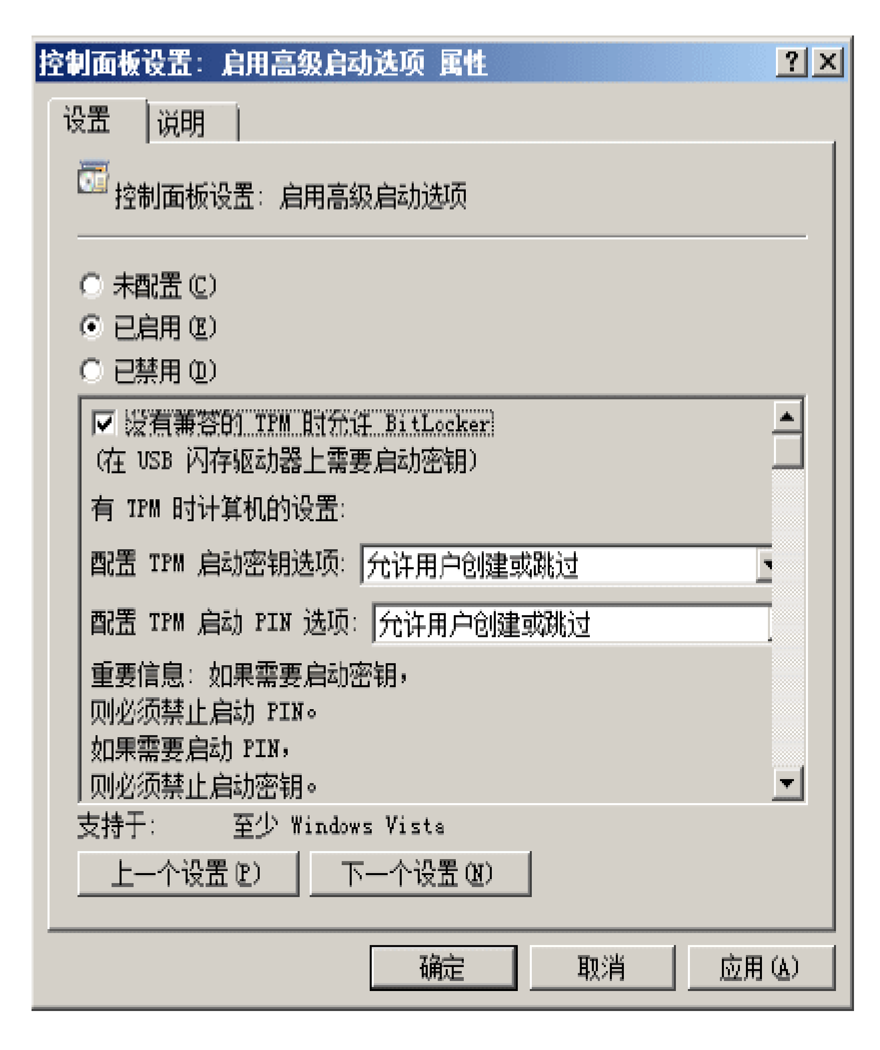


图 18.10　“控制面板设置：启用高级启动选项属性”对话框



注意 Windows Server 2008 系统默认是禁用基于U盘模式的驱动器加密的，通过上述设置即可激活该功能。

03 在“控制面板”窗口中，依次打开“安全”→“BitLocker 驱动器加密”窗口，单击“启用 BitLocker”按钮，显示“BitLocker 驱动器加密平台检查”对话框，如图 18.11 所示。



图 18.11 “BitLocker 驱动器加密平台检查”对话框

04 单击“继续 BitLocker 驱动器加密”按钮，显示“设置 BitLocker 启动首选项”对话框，如图 18.12 所示。由于当前计算机并未集成 TPM 芯片，所以相关选项均显示为“灰色”。

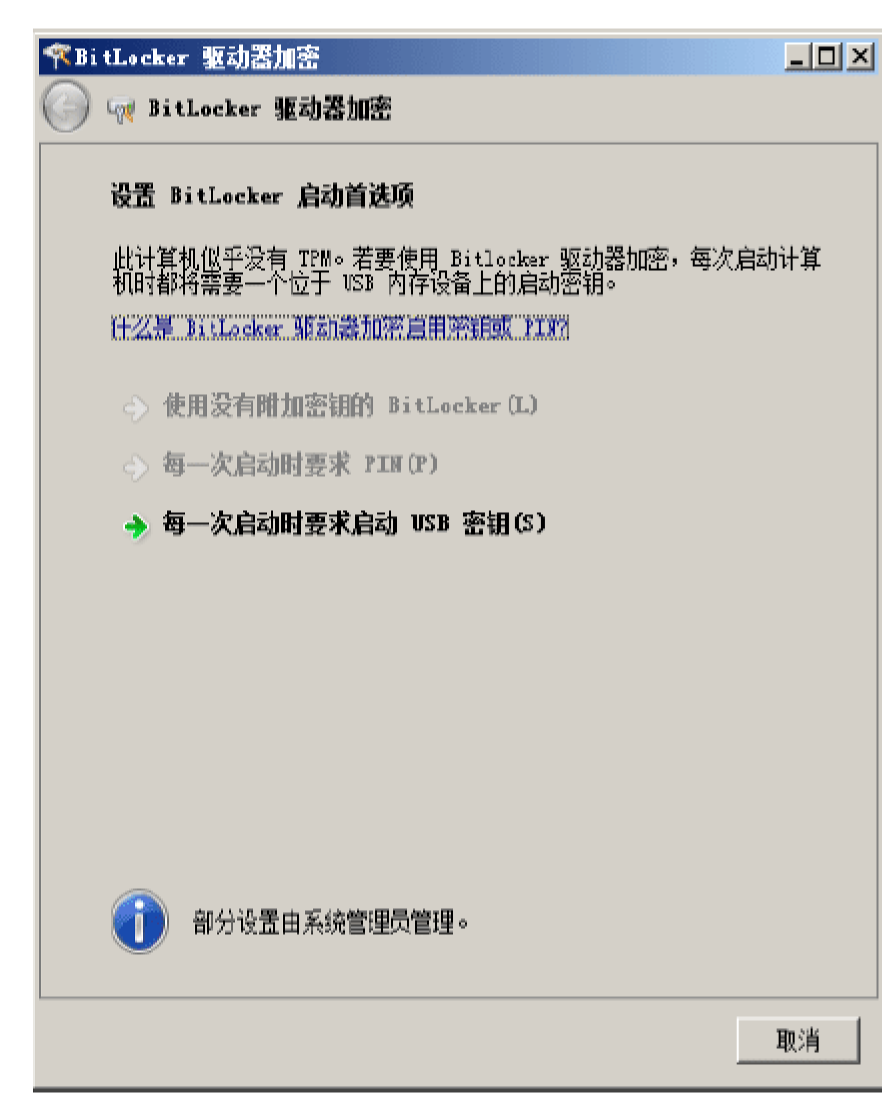


图 18.12 “设置 BitLocker 启动首选项”对话框

05 单击“每一次启动时要求启动 USB 密钥”选项，显示如图 18.13 所示“保存启动密钥”对话框。按照提示，插入事先准备好的U盘即可。

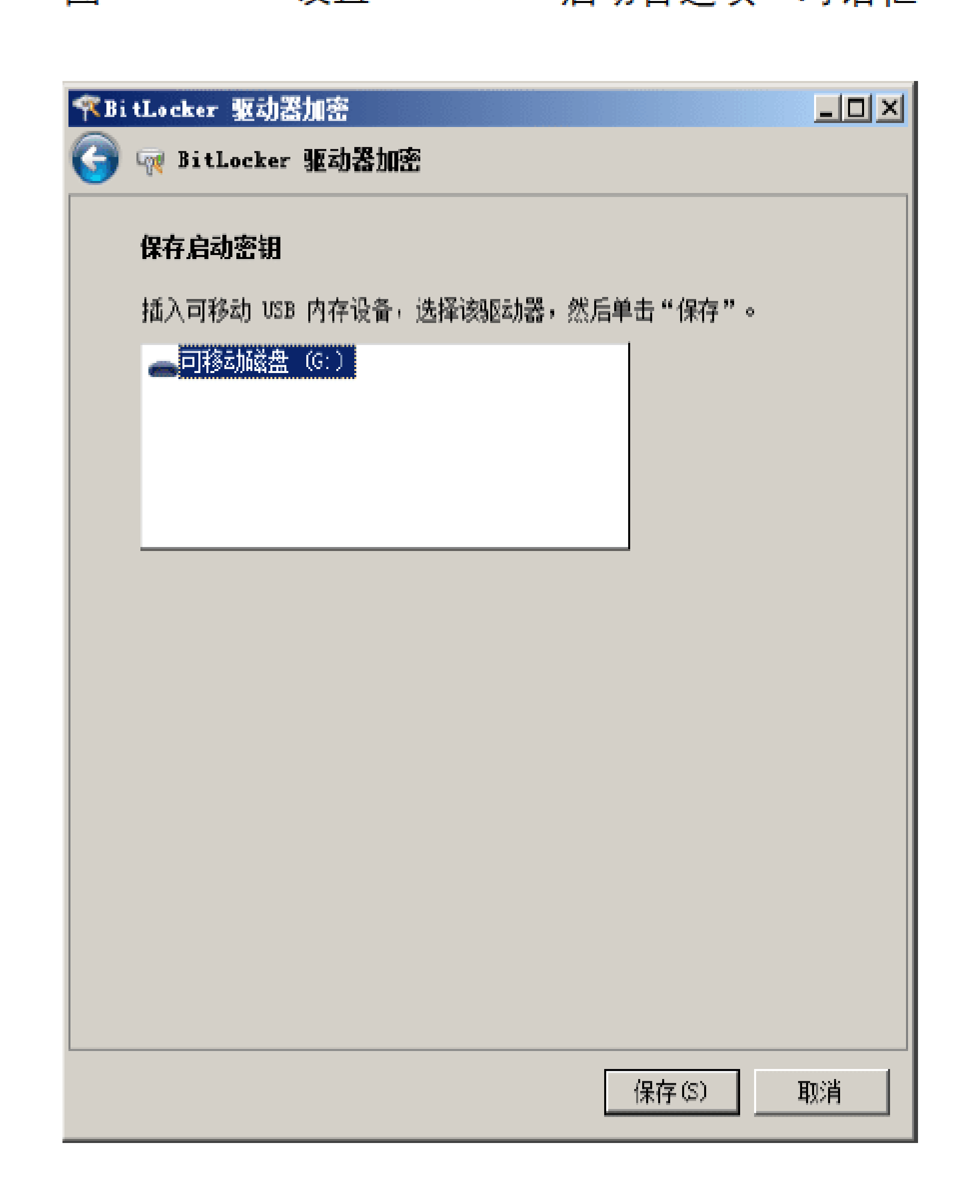


图 18.13 “保存启动密钥”对话框



06 选中 U 盘，单击“保存”按钮，显示如图 18.14 所示“保存恢复密码”对话框。用户可以选择“在 USB 驱动器上保存密码”选项，也可以选择“在文件夹中保存密码”选项，但建议选择“打印密码”选项。此时会再次要求插入 U 盘，单击“保存”按钮，建议将启动密码和恢复密码分开存储，提高安全性。



图 18.14　“保存恢复密码”对话框

07 恢复密码保存成功后，单击“下一步”按钮，显示如图 18.15 所示“加密卷”对话框。默认情况下，BitLocker 会对系统卷进行加密，加密之前将首先进行系统检查。

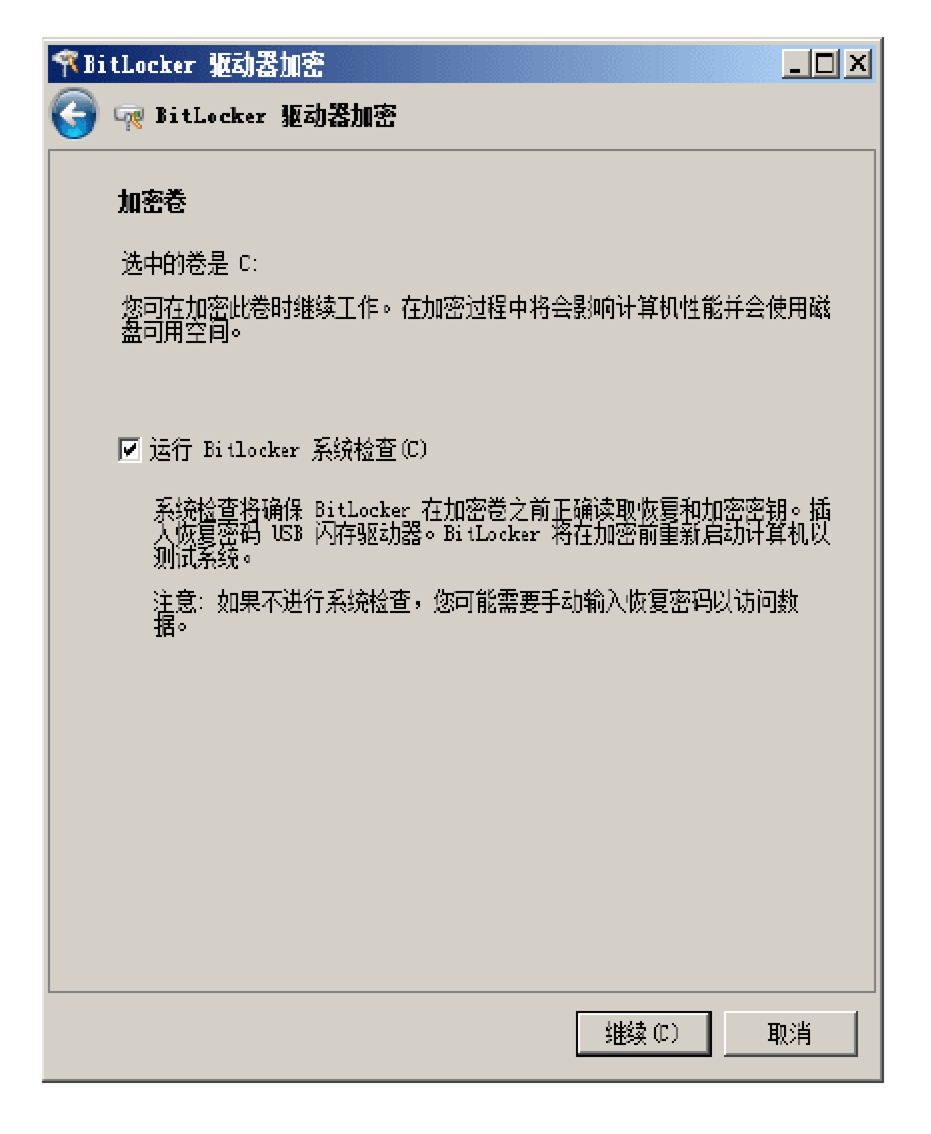


图 18.15　“加密卷”对话框

08 单击“继续”按钮，显示如图 18.16 所示“必须重新启动计算机”对话框，重启时需要插入保存启动密钥的 U 盘，以后每次启动计算机都要用到该 U 盘。



图 18.16　“必须重新启动计算机”对话框

09 单击“现在重启动”按钮，重新启动计算机。重新启动之后，系统将开始进行 BitLocker 加密操作，用户可以在系统托盘处查看具体进度。

使用 BitLocker 加密系统卷完成后，在“服务器管理器”控制台中打开“磁盘管理”窗口，系统卷状态显示为“启动，页面文件，故障转储，逻辑驱动器”，如图 18.17 所示，而“文件系统”也变为“NTFS（BitLocker 已加密）”状态。此时，如果通过其他操作系统读取 Windows Server 2008 的系统所在卷，将被提示“驱动器不可用”，充分保证系统数据的安全。

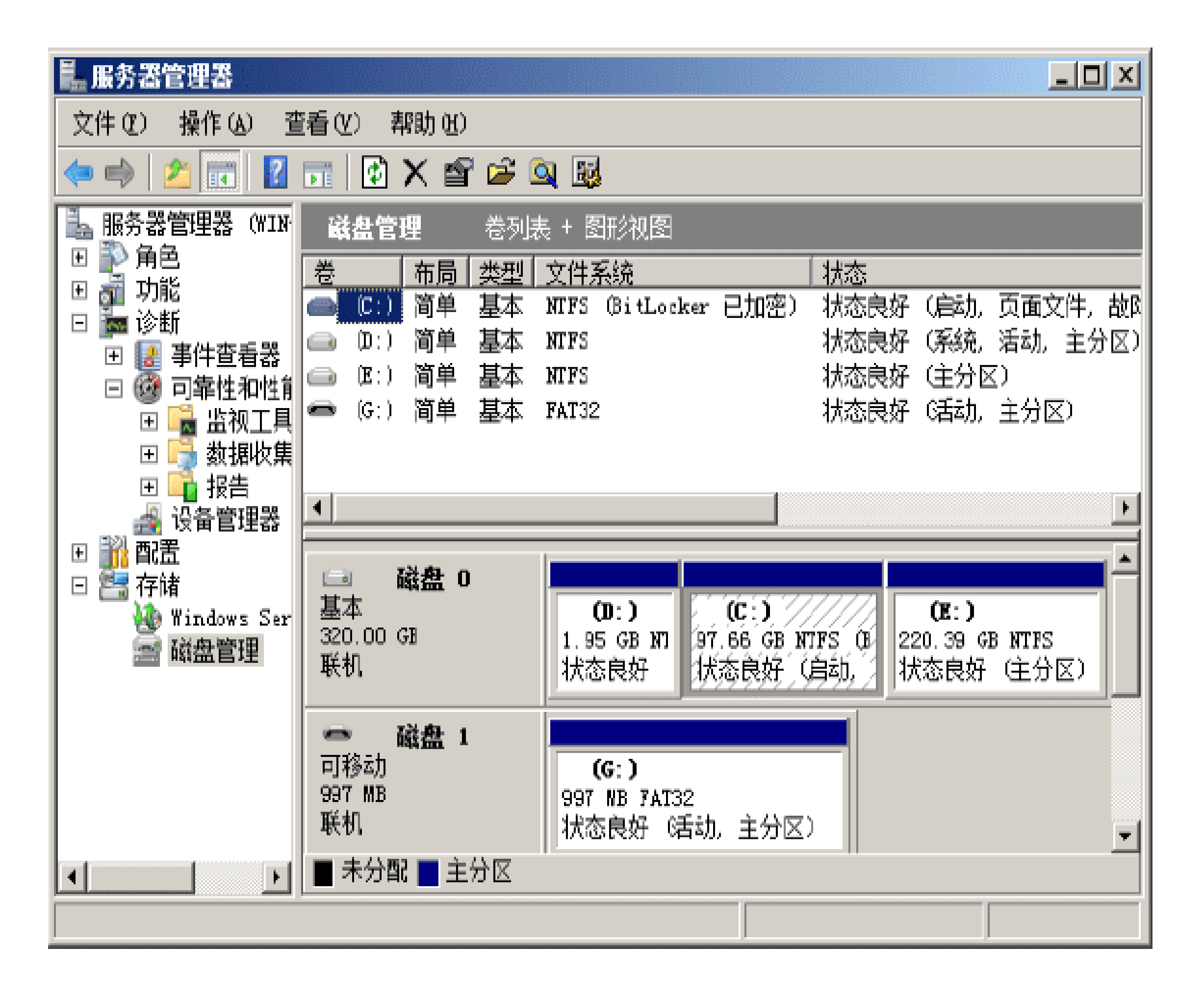


图 18.17　加密后的系统卷

18.1.2　网络访问保护

NAP（网络访问保护，Network Access Protection）是 Windows Server 2008 的一项重要功能，解决客户端无法满足企业安全要求的问题。

1. NAP 方案概述

NAP 系统将网络划分为 4 个部分，即外网、更新服务器组、受限访问区和完全访问区，如图 18.18 所示。

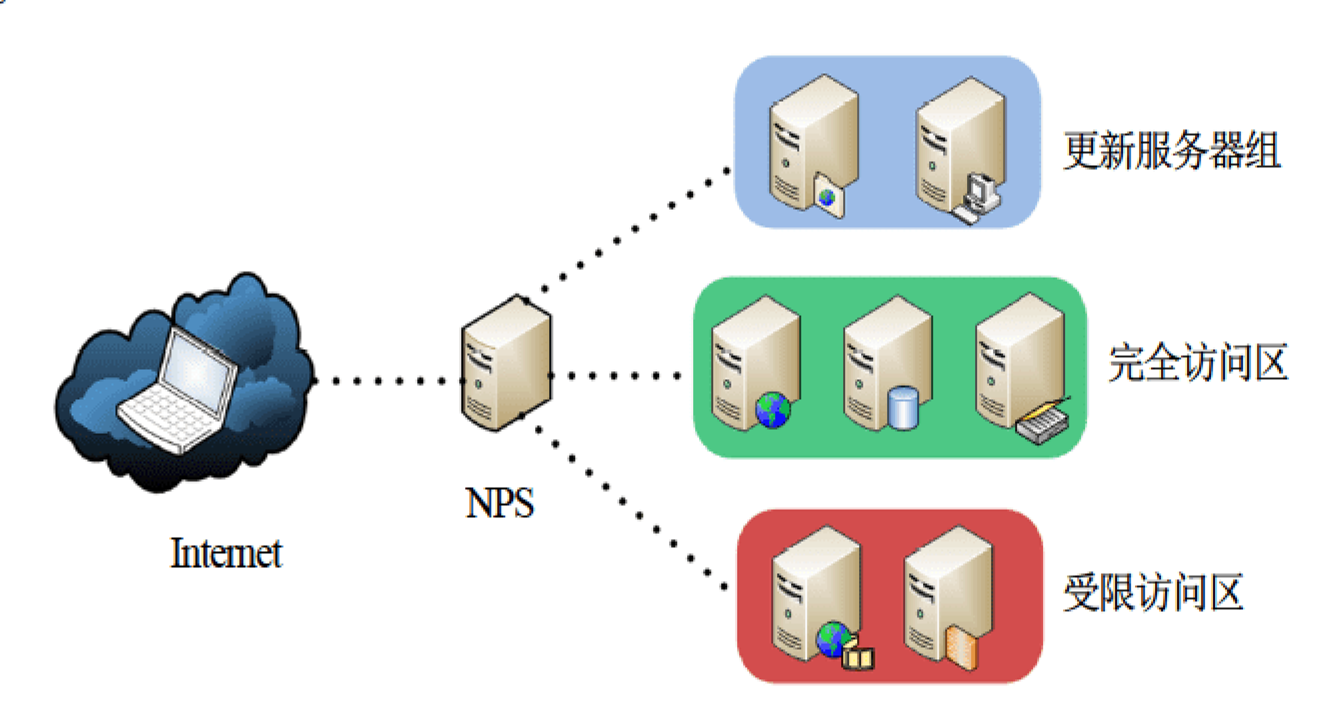


图 18.18　启用 NAP 系统的网络结构

NAP 支持 Windows Vista 和 Windows XP SP3 客户端。客户端第一次连接网络时，首先要验证健康策略，同时将计算机和健康要求策略进行验证，这些健康要求策略由各种 SHAs 和系统健康验证器（System health validators，SHVs）定义。如果计算机符合要求，可以通过多种方式授予计算机完全访问的权限。不符合健康要求的计算机则被授予受限访问权限。另一种方法是允许计算机完全访问，但将计算机标记为不符合健康要求，在只监视环境内使用 NAP 的情况下，可能会用到此方法。为不符合要求的计算机定义的受限访问网络有些情况下是限制连接，有些情况下是限制连接的时间。启用受限网络之后，首先选择受限网络的限制项目，这样



客户端才可以访问修复服务器和健康更新资源来更新客户端的健康状况。也就意味着这些服务器/资源必须是受限网络可用的。

如果客户端不支持 NAP，也不符合健康要求，则需要通过其他方法使其符合健康要求。若正在使用“仅监视”NAP 模式，客户端具有完全访问权限，用户可以继续发送客户端更新，使客户端符合健康要求。若正在使用受限访问 NAP 模式，则只有更新之后，客户端才具有完全访问权限。这里应该注意的是，NAP 不是更新客户端的方法。获取修补程序、恶意软件定义、病毒定义更新之后，可以使用系统中心配置管理器（System Center Configuration Manger，SCCM）或组策略和 WSUS 等解决方案自动更新客户端。

客户端和 NPS 策略服务器之间的多个网络访问技术都需要和 NAP 服务器进行通信，以控制访问。例如，使用 Windows Server 2008 DHCP 服务和 VPN。其他网络访问组件的访问控制依赖 RADIUS，无需使用新版 NAP。充当 RADIUS 客户端的所有组件都要验证客户端请求访问的健康状况，RADIUS 响应控制被授予的权限。

2. NAP 部署注意事项

若当前网络中有多台计算机都是不符合健康要求的，则以受限访问模式启用 NAP 将会导致大部分计算机无法通信。

实现 NAP 的最好方式是在不同阶段使用 NAP 的不同模式。首先在实验室环境内进行测试，然后在生产环境内进行真实试验，但一开始要局限于精通 IP 通信的少量用户和计算机，例如 IT 部门的人员。然后将实验扩展到包含各个部门和科室的所有用户，保证此项技术可以在所有环境内实施。其中来自财务科和 IT 部门的人员使用该技术的方式会有所不同。实验完成后，注销所有部门和科室的员工，然后就可以在整个企业内部署 NAP。

此外，还要测试如何处理异常情况。例如在存在 Linux 客户端或 Windows 2000 系统的网络中，不可以拒绝不支持 NAP 的计算机。测试过程中应注意如下事项：

- 可以根据现有规则定义 NAP 异常；
- 计算机无法兼容 NAP 时，排除此计算机，授予完全访问的权限；
- 可以为来宾计算机定义规则，而这些规则基于计算机是否是企业域的组成部分；
- 可以根据特定计算机的 MAC 地址，为来宾计算机定义规则；
- 对于内部计算机异常来说，可以根据组成员关系定义异常，即策略支持的所有标准。

在设计和部署 NAP 系统时，应考虑如下因素：

- 确定网络中的所有计算机和设备是否都支持 NAP 功能，以及是否确实需要 NAP 保护系统；
- 部署过程中确保重要应用不被中断，以及部署之后确保部分计算机永远可以畅通访问；
- 配置需要检测的安全项目。首先检查防火墙状态，防病毒更新状态。必要时可以创建自定义系统健康代理或验证程序。例如，客户端需要检测是否安装了可以删除机密信息的可移动媒体。该检测只能通过注册表内的全局唯一标识符（Globally Unique Identifier，GUI）实现；

■ 网络中的临时用户包括多种类型，应注意为不同类型的用户设置不同类型的访问。如果部署 IPSec 强制，则必须创建多个外网。如果部署 802.1x 强制，则需要创建多个 VLAN；
■ 确保不符合健康要求的客户端可以访问更新服务器组。

18.1.3 用户帐户控制

管理员帐户对本地系统拥有完全控制权限。通常情况下，为了确保系统安全，禁止赋予其他帐户过高的操作权限。此时，如果管理员帐户发生故障，只有其他用户帐户可用，则会导致要求管理员权限才可以执行的操作无法顺利完成。UAC（User Access Control，用户访问控制）可以保护管理员会话连接，防止出现与管理员帐户特权相关的故障。

UAC 创建了两个管理员令牌，一个令牌具有管理员特权，另一个令牌具有普通凭据。默认情况下，运行管理员会话时使用普通的用户特权，只有需要高级凭据时，提示管理员同意授权使用提升的权利来执行管理功能。非管理员也是如此，运行的功能要求高级特权时，提示用户输入管理员帐户用户名和密码，在不注销用户的情况下，允许管理员提供即时权限提升（Over the Shoulder，OTS）协助。

内置管理员帐户默认禁用管理批准模式（Admin Approval Mode，AAM），所以管理员无法看到授予管理员权限的提示，但 UAC 仍然是 Windows Server 2008 的一部分。例如，域管理员（不是内置域管理员）尝试修改服务器时间时，显示如图 18.19 所示"用户帐户控制"对话框。屏幕的其他部分显示为灰色，这正是 UAC 的安全功能，防止恶意软件干扰 UAC 提示。

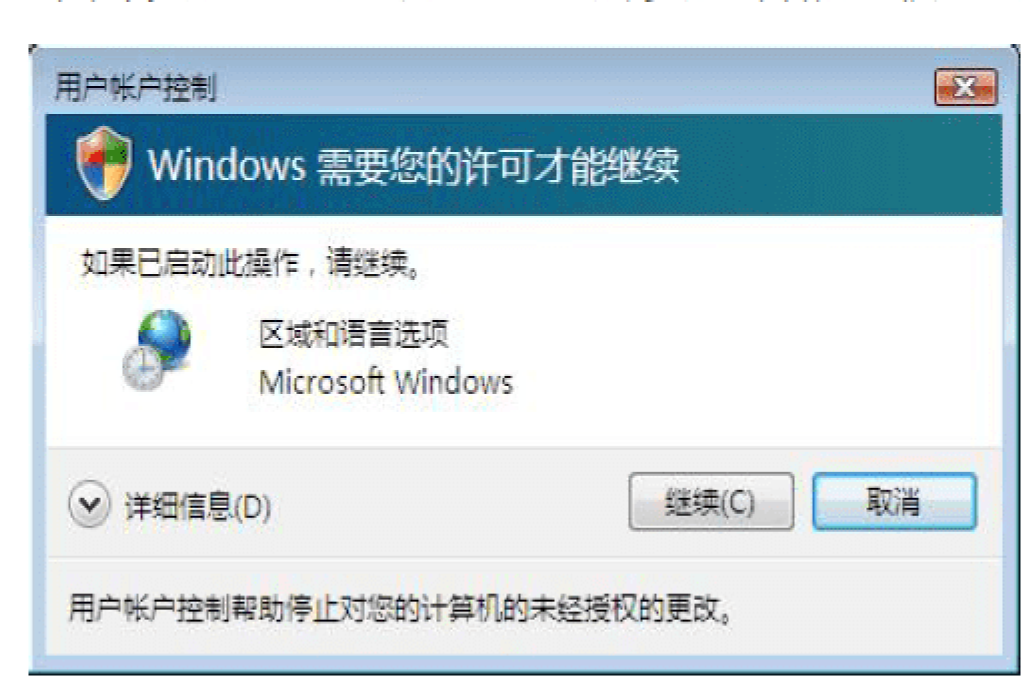


图 18.19 "用户帐户控制"对话框

手动配置 UAC 的方式很多，使用组策略设置可以实现更准确的控制。依次单击"计算机配置"→"策略"→"Windows 设置"→"安全设置"→"本地策略"→"安全选项"，就可以看到这些设置，而且这些设置和服务器本地计算机策略中的本地设置相同，此处不再赘述。

18.1.4 高级安全 Windows 防火墙

Windows Server 2008 中的高级安全 Windows 防火墙是一款基于状态主机的防火墙软件，可根据自身配置和正在运行的应用来决定允许或阻止网络流量，从而保护网络免遭恶意用户和



程序的侵害。高级安全 Windows 防火墙的安全功能包括进出流量筛选、通过 MMC 控制台管理本地或远程防火墙、IPSec 连接规则等。

1. 双向数据包拦截

Windows Server 2008 系统中高级安全 Windows 防火墙会拦截所有非请求进入的流量，包括不符合发送响应的流量，或者通过例外允许的非请求流量。这是防火墙功能的重要组成部分，可避免计算机受到非请求进入流量中的病毒和蠕虫的影响。

Windows Server 2008 中 Windows 防火墙的默认行为是：

- 除非抵达流量是响应发送请求的或匹配于已配置的例外，否则将阻挡所有抵达流量；
- 除非发送流量匹配于已配置的例外，否则将允许所有发送流量。

2. MMC 管理方式

控制台管理是 Windows Server 2008 系统的一大特色，其中高级安全 Windows 防火墙也可以通过 MMC 管理，另外，通过 MMC 还可以管理远程计算机上的 Windows 防火墙（目前的 Windows 防火墙只有通过远程桌面连接才能做到）。

除此之外，管理员还可以通过组策略和命令行方式配置 Windows 防火墙。

3. 集成防火墙和 IPSec 设置

IPSec 是一组用于为 IP 流量提供加密保护的 Internet 标准。在先前版的 Windows Server 系统中，管理员需要分别配置 Windows 防火墙和 IPSec。由于 Windows 中的主机防火墙和 IPsec 都可以允许或阻止流量进入网络，因此难免会产生重叠或彼此矛盾的情况。新的 Windows 防火墙在统一的 GUI 和命令行命令中将这两种网络服务配置结合在一起。集成防火墙和 IPsec 设置可简化 IPsec 的配置。

通常情况下，配置 IPsec 后，只允许使用 IPsec 加密的服务器进行通信，保证安全访问，这也是 NAP 的基础。要求配置 IPsec 时，只有计算机成为受信任基础设施之后才可以进行通信，也就是所谓的域隔离，意味着只有域成员可以参与 IPsec 通信。此外，也可以使用 IPsec 配置，实现服务器隔离。例如，SQL 服务器上包含重要的数据信息，此时可以配置 IPsec，只允许域成员或指定计算机与该服务器通信。

4. 配置防火墙例外的几种方法

Windows Server 2008 中的高级安全功能，允许管理员通过各种方法配置防火墙的例外：

- 根据 IP 协议号配置例外。高级安全 Windows 防火墙允许管理员根据名称选择协议，也可以就特定的流量手工输入 IPv4 协议值或 IPv6 Next Header 字段名称；
- 根据源和目的地配置例外。管理员可以针对进出防火墙的流量配置源和目的地 TCP 或 UDP 端口，进一步明确允许或禁止哪种类型的 TCP 和 UDP 流量；
- 可就所有端口或多个端口配置例外。管理员还可以指定所有 TCP 或 UDP 端口（用于所

有 TCP 或所有 UDP 流量）或列出用逗号分隔的多个端口列表；

- 根据特定接口类型配置例外。管理员可以指定应用于所有接口或特定接口类型的（如 LAN、远程访问或无线接口等）例外；
- 根据类型和代码配置 ICMP 流量例外。Windows Server 2008 中的 Windows 防火墙预设了常见的 ICMP 和 ICMP v6 消息例外，管理员可指定 ICMP 或 ICMP v6 类型和代码字段值来添加新的 ICMP 和 ICMPv6 消息；
- 根据服务配置例外。管理员可以指定例外应用于任何进程、仅应用于服务或根据服务名称应用于特定服务等。此外，管理员也可以输入服务名称的缩写。例如，如果管理员希望仅就计算机浏览器服务配置例外，那么可从运行在计算机上的服务列表中选择计算机浏览器服务。

18.1.5 其他新增安全特性

除前面提到的常用安全功能之外，Windows Server 2008 系统还提供了多项有助于企业提升服务器安全和网络安全的增强型特性。

1. 代码完整性

当通过登录所有操作系统的可执行文件和 DLL 文件运行操作系统时，代码完整有助于保护操作系统文件。一旦将文件载入内存后即可检验这些文件的有效性。

2. Windows Service Hardening

Windows Service Hardening 能够防止关键 Windows 服务被文档系统、注册表或网络中的异常活动使用，从而确保系统具有更高的安全性。由于 Windows Service Hardening 默认运行的服务很少，而且服务帐户拥有的特权极小，因而限制了网络访问。

3. 限制可移动设备安装

Windows Server 2008 为企业提供一种保护数据的方法，这种方法可以防止数据被拷贝到 U 盘等可移动设备上。通过配置组策略（Group Policy）可实现对键盘、鼠标或者 U 盘的控制。管理者在决定移动设备如何使用方面有着充分的灵活性，包括：

- 防止用户安装任何设备；
- 允许用户仅安装“许可列表”上的设备；
- 防止用户安装“禁止列表”上的设备；
- 对于指定设备拒绝用户读取或者写入。

限制可移动设备安装不仅有助于降低数据被盗风险，而且还能进一步降低支持成本，因为这样可确保用户仅安装调整并配备了支持型帮助桌面的设备。



18.2　升级的安全特性

Windows Server 2008 系统除新增了多项安全功能之外，还对原有安全特性进行了升级和扩展，可以为用户提供更高级、更全面的安全防护。例如 Windows Server 2008 中的组策略就是变化较大的组件之一，不仅新增了多项安全策略，而且划分更加详细，满足管理员安全管理的各种需求。类似的升级型安全特性还包括事件查看器、可靠性和性能监视器等组件。

18.2.1　组策略管理

Windows Server 2008 中的组策略提供了全新的管理方法，并且增加了多项实用管理类别。Windows Server 2008 中组策略的新增管理功能如下：

- 通过电源选项实现的成本节约。在 Windows Server 2008 中，所有电源选项都已启用组策略，从而实现潜在的巨大成本节约。通过组策略控制电源选项可能会使企业节省大量资金。用户可以通过单个组策略设置修改特定的电源选项，或者构建可使用组策略部署的自定义电源计划；
- 阻止设备安装的功能。在 Windows Server 2008 中，用户可以集中限制在企业的计算机上安装指定类型的硬件设备，例如 USB 设备、CD-RW 驱动器、DVD-RW 驱动器以及其他可移动介质等；
- 改进的安全设置。在 Windows Server 2008 中，将防火墙和 IPSec 组策略设置组合在一起，使用户无需创建和维护重复的功能即可利用两种技术的优势。这些组合的防火墙和 IPSec 策略设置所支持的一些方案是 Internet 上安全的服务器到服务器的通信，这些方案会根据信任关系或计算机的运行状况限制对域资源的访问,并且保护到特定服务器的数据通信，使之符合数据隐私和安全性的法规要求；
- 扩展的 Internet Explorer 设置管理。在 Windows Server 2008 中，用户可以打开和编辑 IE 组策略设置，而没有根据管理工作站的配置无意中改变策略设置状态的风险；
- 基于位置的打印机指定。在 Windows Server 2008 中，用户可以基于站点位置指定打印机。当移动用户移动到另一个位置时，组策略可以针对新的位置更新其打印机。回到其主位置的移动用户可以看到其打印机仍为惯用的默认打印机；
- 将打印机驱动程序安装委派给用户。在 Windows Server 2008 中，管理员可以使用组策略将安装打印机驱动程序的能力委派给用户。该功能通过限制管理凭据的分发来维护安全性。

18.2.2　服务器安全配置向导

默认情况下，Windows Server 2008 系统并非十分安全，许多安全配置和功能并未启用。通过服务器管理器安装角色、角色服务和功能时，将会自动配置特定服务器配置的安全设置。

但是，不能使用服务器管理器自定义更改安全设置。借助服务器安全配置向导（SCW），管理员可以对系统默认设置进行更改，例如为特定服务器角色配置防火墙规则等。在 Windows Server 2008 系统中，用户仍可以使用 SCW 创建和应用服务器安全策略，但是在大多数情况下，不需要使用 SCW 即可在安装时保护服务器的安全。

在最初的服务器角色安装后，可以使用 SCW 检查服务器配置是否随着时间的变化产生了漏洞，并按要求对策略设置进行更新来保护服务器的安全。用户可以在下列情况下使用 SCW 创建并应用服务器的安全策略：

- 在 Windows Server 2008 计算机上修改默认组件的配置。在更改未通过服务器管理器安装的组件配置时，需要使用 SCW 更新服务器的安全策略；
- 为未通过服务器管理器安装的服务器角色（例如 SQL Server 或 Exchange Server）创建并应用策略。SCW 包含许多无法使用服务器管理器安装的服务器角色和功能；
- 为非 Microsoft 应用程序定义新的角色，并为这些角色创建和应用策略。SCW 具有一个组织可用来创建新角色的公共架构。在添加或删除非 Microsoft 应用程序时运行 SCW。

在中小型企业网络中，可以使用 SCW 中的默认设置快速创建安全策略，帮助基于其角色保护服务器的安全并确保安全设置为最新状态。还可以将使用“安全模板”管理单元创建的自定义安全模板导入到 SCW 策略中。这样便允许包含除 SCW 设置之外的其他设置。然后使用该向导将 SCW 策略应用到本地计算机中，也可以使用组策略将其应用到许多计算机中。

18.2.3 安全配置和分析

用户可以使用安全配置和分析管理单元，将本地计算机策略与分析数据库进行比较，从而确定数据库中所需设置是否与本地策略之间存在差异。还可以使用现有的数据库，或导入希望使用的一个或多个安全模板，使用更新的设置创建新的数据库。分析结果中会提供针对当前系统设置的一些建议，并标注当前设置与建议的安全级别不一致的地方，以便用户改进。

1. 安全模板

安全模板是安全配置和分析的核心，提供要配置的设置。第一次打开“安全模板”管理单元时，只能看到一个登录用户的文档文件夹，而且文件夹内没有任何模板，但可以在这里创建自己的模板。

Windows Server 2008 提供了大量模板，这些模板可以在%windir%\security\templates 文件夹内找到。其中有两个模板可以帮助定义服务器的初始配置、独立配置域控制器。早期操作系统中添加的额外模板在 Windows Server 2008 中也可以使用。Windows Server 2008 默认提供的安全模板如下：

- SecureWS：适用于具有安全设置的工作站和服务器；
- SecureDC：适用于安全环境中的域控制器；
- HiSecWS：适用于安全配置要求非常高的工作站和服务器；

但是，不能使用服务器管理器自定义更改安全设置。借助服务器安全配置向导（SCW），管理员可以对系统默认设置进行更改，例如为特定服务器角色配置防火墙规则等。在 Windows Server 2008 系统中，用户仍可以使用 SCW 创建和应用服务器安全策略，但是在大多数情况下，不需要使用 SCW 即可在安装时保护服务器的安全。

在最初的服务器角色安装后，可以使用 SCW 检查服务器配置是否随着时间的变化产生了漏洞，并按要求对策略设置进行更新来保护服务器的安全。用户可以在下列情况下使用 SCW 创建并应用服务器的安全策略：

- 在 Windows Server 2008 计算机上修改默认组件的配置。在更改未通过服务器管理器安装的组件配置时，需要使用 SCW 更新服务器的安全策略；
- 为未通过服务器管理器安装的服务器角色（例如 SQL Server 或 Exchange Server）创建并应用策略。SCW 包含许多无法使用服务器管理器安装的服务器角色和功能；
- 为非 Microsoft 应用程序定义新的角色，并为这些角色创建和应用策略。SCW 具有一个组织可用来创建新角色的公共架构。在添加或删除非 Microsoft 应用程序时运行 SCW。

在中小型企业网络中，可以使用 SCW 中的默认设置快速创建安全策略，帮助基于其角色保护服务器的安全并确保安全设置为最新状态。还可以将使用“安全模板”管理单元创建的自定义安全模板导入到 SCW 策略中。这样便允许包含除 SCW 设置之外的其他设置。然后使用该向导将 SCW 策略应用到本地计算机中，也可以使用组策略将其应用到许多计算机中。

18.2.3 安全配置和分析

用户可以使用安全配置和分析管理单元，将本地计算机策略与分析数据库进行比较，从而确定数据库中所需设置是否与本地策略之间存在差异。还可以使用现有的数据库，或导入希望使用的一个或多个安全模板，使用更新的设置创建新的数据库。分析结果中会提供针对当前系统设置的一些建议，并标注当前设置与建议的安全级别不一致的地方，以便用户改进。

1. 安全模板

安全模板是安全配置和分析的核心，提供要配置的设置。第一次打开“安全模板”管理单元时，只能看到一个登录用户的文档文件夹，而且文件夹内没有任何模板，但可以在这里创建自己的模板。

Windows Server 2008 提供了大量模板，这些模板可以在%windir%\security\templates 文件夹内找到。其中有两个模板可以帮助定义服务器的初始配置、独立配置域控制器。早期操作系统中添加的额外模板在 Windows Server 2008 中也可以使用。Windows Server 2008 默认提供的安全模板如下：

- SecureWS：适用于具有安全设置的工作站和服务器；
- SecureDC：适用于安全环境中的域控制器；
- HiSecWS：适用于安全配置要求非常高的工作站和服务器；

但是，不能使用服务器管理器自定义更改安全设置。借助服务器安全配置向导（SCW），管理员可以对系统默认设置进行更改，例如为特定服务器角色配置防火墙规则等。在 Windows Server 2008 系统中，用户仍可以使用 SCW 创建和应用服务器安全策略，但是在大多数情况下，不需要使用 SCW 即可在安装时保护服务器的安全。

在最初的服务器角色安装后，可以使用 SCW 检查服务器配置是否随着时间的变化产生了漏洞，并按要求对策略设置进行更新来保护服务器的安全。用户可以在下列情况下使用 SCW 创建并应用服务器的安全策略：

- 在 Windows Server 2008 计算机上修改默认组件的配置。在更改未通过服务器管理器安装的组件配置时，需要使用 SCW 更新服务器的安全策略；
- 为未通过服务器管理器安装的服务器角色（例如 SQL Server 或 Exchange Server）创建并应用策略。SCW 包含许多无法使用服务器管理器安装的服务器角色和功能；
- 为非 Microsoft 应用程序定义新的角色，并为这些角色创建和应用策略。SCW 具有一个组织可用来创建新角色的公共架构。在添加或删除非 Microsoft 应用程序时运行 SCW。

在中小型企业网络中，可以使用 SCW 中的默认设置快速创建安全策略，帮助基于其角色保护服务器的安全并确保安全设置为最新状态。还可以将使用“安全模板”管理单元创建的自定义安全模板导入到 SCW 策略中。这样便允许包含除 SCW 设置之外的其他设置。然后使用该向导将 SCW 策略应用到本地计算机中，也可以使用组策略将其应用到许多计算机中。

18.2.3 安全配置和分析

用户可以使用安全配置和分析管理单元，将本地计算机策略与分析数据库进行比较，从而确定数据库中所需设置是否与本地策略之间存在差异。还可以使用现有的数据库，或导入希望使用的一个或多个安全模板，使用更新的设置创建新的数据库。分析结果中会提供针对当前系统设置的一些建议，并标注当前设置与建议的安全级别不一致的地方，以便用户改进。

1. 安全模板

安全模板是安全配置和分析的核心，提供要配置的设置。第一次打开“安全模板”管理单元时，只能看到一个登录用户的文档文件夹，而且文件夹内没有任何模板，但可以在这里创建自己的模板。

Windows Server 2008 提供了大量模板，这些模板可以在%windir%\security\templates 文件夹内找到。其中有两个模板可以帮助定义服务器的初始配置、独立配置域控制器。早期操作系统中添加的额外模板在 Windows Server 2008 中也可以使用。Windows Server 2008 默认提供的安全模板如下：

- SecureWS：适用于具有安全设置的工作站和服务器；
- SecureDC：适用于安全环境中的域控制器；
- HiSecWS：适用于安全配置要求非常高的工作站和服务器；

但是，不能使用服务器管理器自定义更改安全设置。借助服务器安全配置向导（SCW），管理员可以对系统默认设置进行更改，例如为特定服务器角色配置防火墙规则等。在 Windows Server 2008 系统中，用户仍可以使用 SCW 创建和应用服务器安全策略，但是在大多数情况下，不需要使用 SCW 即可在安装时保护服务器的安全。

在最初的服务器角色安装后，可以使用 SCW 检查服务器配置是否随着时间的变化产生了漏洞，并按要求对策略设置进行更新来保护服务器的安全。用户可以在下列情况下使用 SCW 创建并应用服务器的安全策略：

- 在 Windows Server 2008 计算机上修改默认组件的配置。在更改未通过服务器管理器安装的组件配置时，需要使用 SCW 更新服务器的安全策略；
- 为未通过服务器管理器安装的服务器角色（例如 SQL Server 或 Exchange Server）创建并应用策略。SCW 包含许多无法使用服务器管理器安装的服务器角色和功能；
- 为非 Microsoft 应用程序定义新的角色，并为这些角色创建和应用策略。SCW 具有一个组织可用来创建新角色的公共架构。在添加或删除非 Microsoft 应用程序时运行 SCW。

在中小型企业网络中，可以使用 SCW 中的默认设置快速创建安全策略，帮助基于其角色保护服务器的安全并确保安全设置为最新状态。还可以将使用“安全模板”管理单元创建的自定义安全模板导入到 SCW 策略中。这样便允许包含除 SCW 设置之外的其他设置。然后使用该向导将 SCW 策略应用到本地计算机中，也可以使用组策略将其应用到许多计算机中。

18.2.3 安全配置和分析

用户可以使用安全配置和分析管理单元，将本地计算机策略与分析数据库进行比较，从而确定数据库中所需设置是否与本地策略之间存在差异。还可以使用现有的数据库，或导入希望使用的一个或多个安全模板，使用更新的设置创建新的数据库。分析结果中会提供针对当前系统设置的一些建议，并标注当前设置与建议的安全级别不一致的地方，以便用户改进。

1. 安全模板

安全模板是安全配置和分析的核心，提供要配置的设置。第一次打开“安全模板”管理单元时，只能看到一个登录用户的文档文件夹，而且文件夹内没有任何模板，但可以在这里创建自己的模板。

Windows Server 2008 提供了大量模板，这些模板可以在%windir%\security\templates 文件夹内找到。其中有两个模板可以帮助定义服务器的初始配置、独立配置域控制器。早期操作系统中添加的额外模板在 Windows Server 2008 中也可以使用。Windows Server 2008 默认提供的安全模板如下：

- SecureWS：适用于具有安全设置的工作站和服务器；
- SecureDC：适用于安全环境中的域控制器；
- HiSecWS：适用于安全配置要求非常高的工作站和服务器；



■ HiSecDC：适用于安全配置要求非常高的工作站和服务器。

使用安全模板添加搜索安全模板的额外路径时，选择“新安全模板搜索路径”操作。此外，如果安装了解决方案加速器，例如包含额外安全模板的 Windows Server 2008 安全指南，可以添加解决方案加速器的位置。

打开安全模板，查看配置的设置，需要修改设置时，不是修改操作系统提供的模板，而是使用“另存为”操作将模板保存为其他文件名。如图 18.20 所示显示了安全指南模板指定的域密码设置。需要注意的是，只需定义模板设置部分，其他设置都保留为“未定义”状态即可。使用“新建模板”操作可创建一个新模板，并指定模板的名称和描述信息。

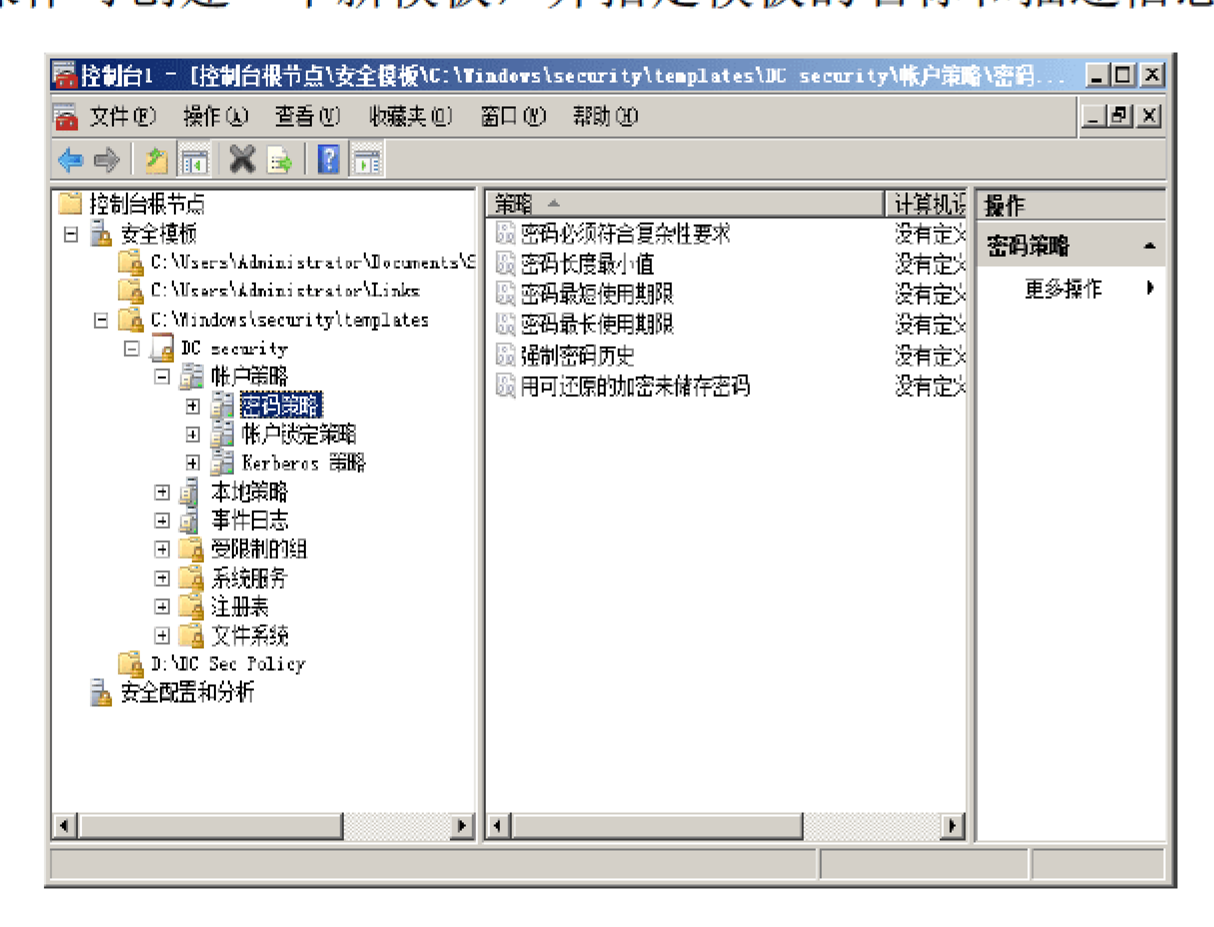


图 18.20　查看模板中定义的设置

2. 使用“安全配置和分析”管理单元

使用“安全配置和分析”管理单元的第一步就是打开存储配置设置信息的安全数据库，选择要使用的安全模板。若不存在安全模板，则创建一个新模板。使用安全模板载入安全模板设置，将模板设置和计算机设置进行对比。“安全配置和分析”管理单元只能在安全数据库中运行，也只有从安全模板将设置导入安全数据库的时候才会用到安全模板。

01 在“安全配置和分析”控制台中，右击“安全配置和分析”节点，在快捷菜单中选择“打开数据库”选项，显示如图 18.21 所示“打开数据库”对话框，选择安全数据库（.sdb）文件。

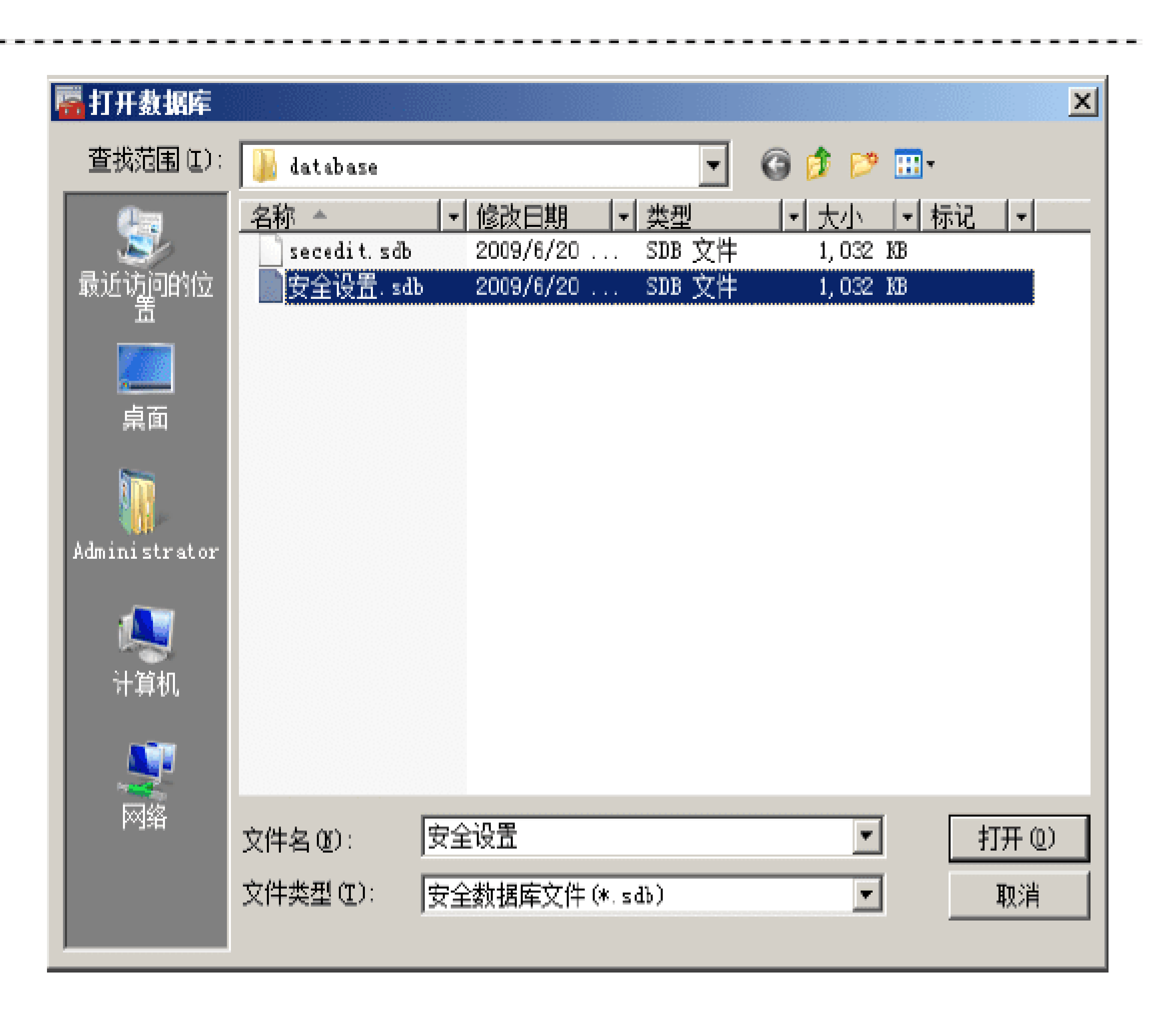


图 18.21　“打开数据库”对话框

02 单击“打开”按钮，显示如图 18.22 所示“安全配置和分析”对话框，显示添加的数据库。

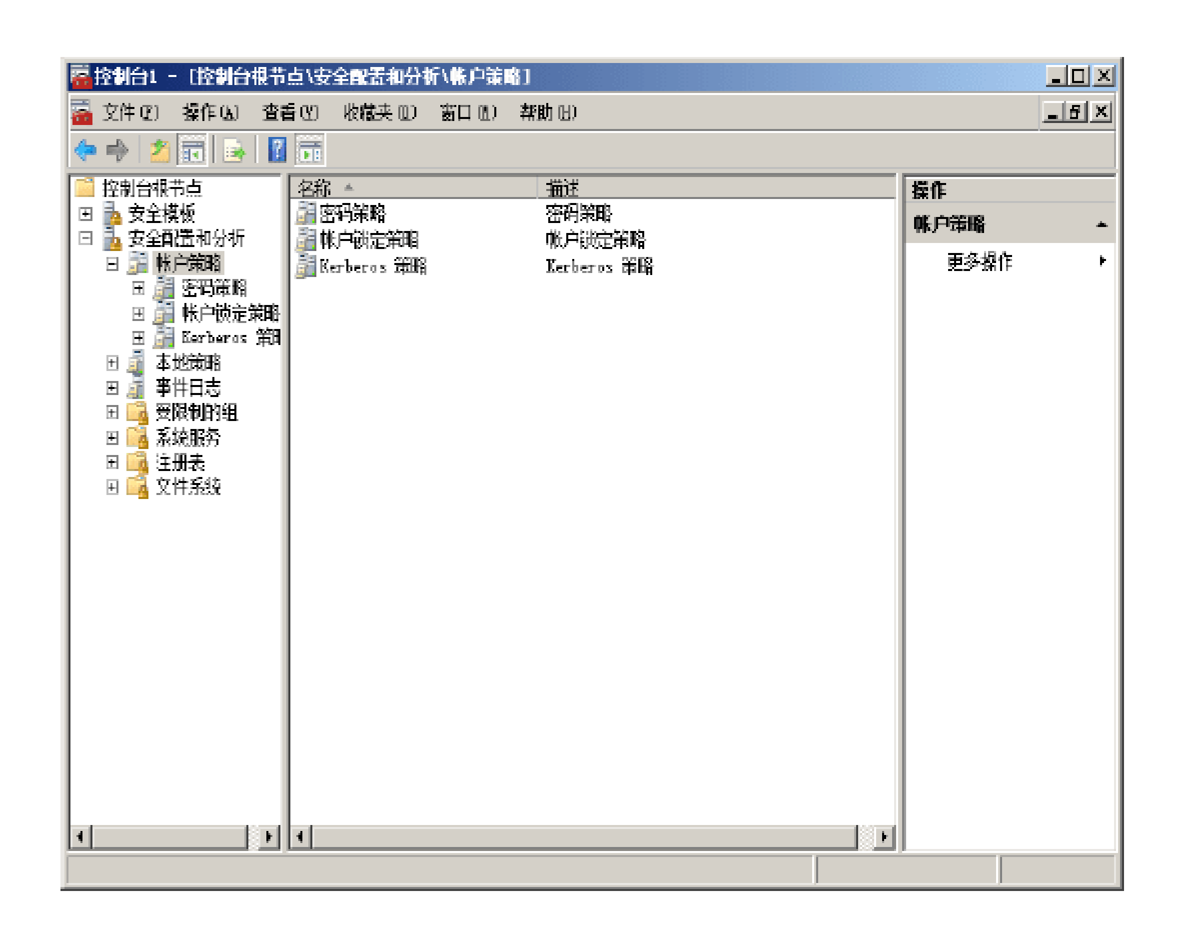


图 18.22　显示添加的数据库

03 右击“安全配置和分析”节点，在快捷菜单中选择“立即配置计算机”选项，显示如图 18.23 所示“配置系统”对话框，选择需要配置的模版。

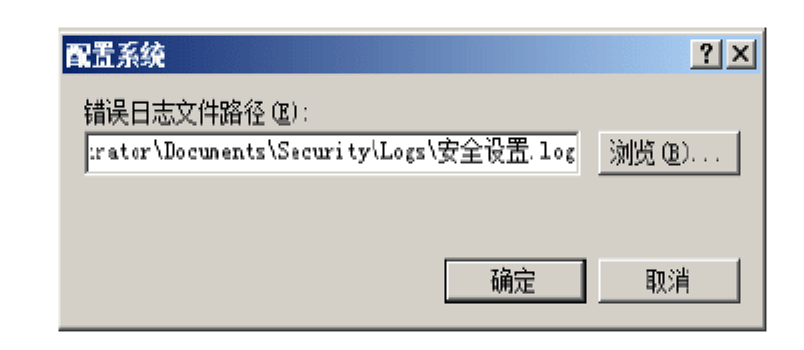


图 18.23　“配置系统”对话框

04 单击“确定”按钮，开始配置计算机安全，主要包括用户权限分配、受限制的组、注册表和文件系统等。配置完成后，将自动显示生成的日志文件，如图 18.24 所示。

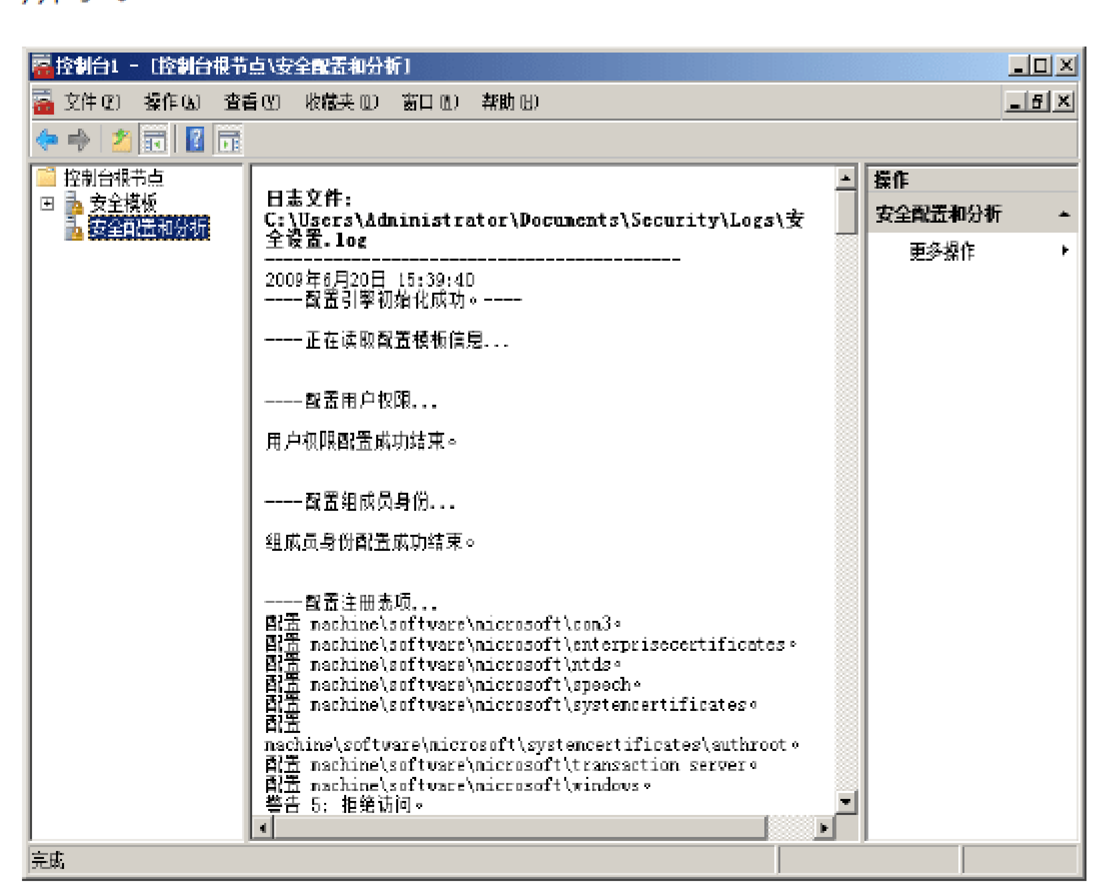


图 18.24　显示日志文件

05 右击“安全配置和分析”节点，在快捷菜单中选择“立即分析计算机”选项，显示如图 18.25 所示“进行分析”对话框，选择要分析的模板。

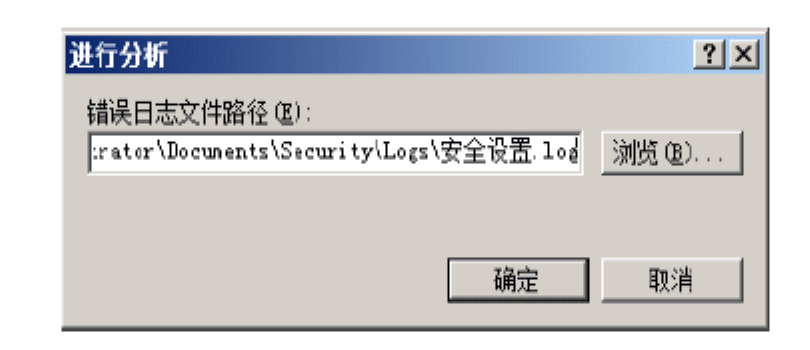


图 18.25　“进行分析”对话框

06 单击“确定”按钮，即可开始分析系统安全机制。完成后，显示如图 18.26 所示的日志信息。

07 查看安全分析结果。分析完成后，展开“安全配置和分析”中的相关节点，即可查看对应的分析结果。如果计算机设置和模板设置匹配，设置图标显示绿色对号；如果计算机设置和模板不匹配，设置图标显示红色错号，如图 18.27 所示。如果某项计算机设置没有在模板中定义，策略图标不显示对号或错号，数据库设置显示为“没有定义”。





图 18.26　显示日志文件



图 18.27　计算机设置和模板设置是否匹配

18.2.4　Windows 事件订阅与收集

Windows Server 2008 的事件查看器也是变化较大的系统组件之一，其中事件订阅就是一项非常重要的新增功能，允许管理员订阅来自远程 Windows 系统（Windows Vista 或 Windows Server 2008）的事件日志。通过它，管理员可以轻松做到集中分析和监控计算机的状态。订阅功能依赖于 Windows 远程管理（WinRM）服务和 Windows 事件收集器（Wecsvc）服务，这两项服务必须在参与转发和收集过程的计算机上运行，目前只有运行 Windows Server 2008 和 Windows Vista 操作系统的计算机支持此功能。

1. 配置源计算机

所谓源计算机就是指事件的真正来源，此处以 Windows Vista 系统为例，需要在源计算机上开启远程管理功能，即允许收集服务器通过网络登录并管理该计算机。需要注意的是，源计算机和事件收集服务器必须隶属于同一域，或建立在信任关系的不同域中。

01 以管理员登录系统，在命令提示符窗口中，输入如下命令：

```
winrm quickconfig
```

按 Enter 键执行，显示如图 18.28 所示结果。提示目前该计算机没有设置成为允许远程访问，执行更改后，即可接受远程访问，问是否继续。

02 输入 Y 并按 Enter 键执行，表示确认更改，显示如图 18.29 所示结果。

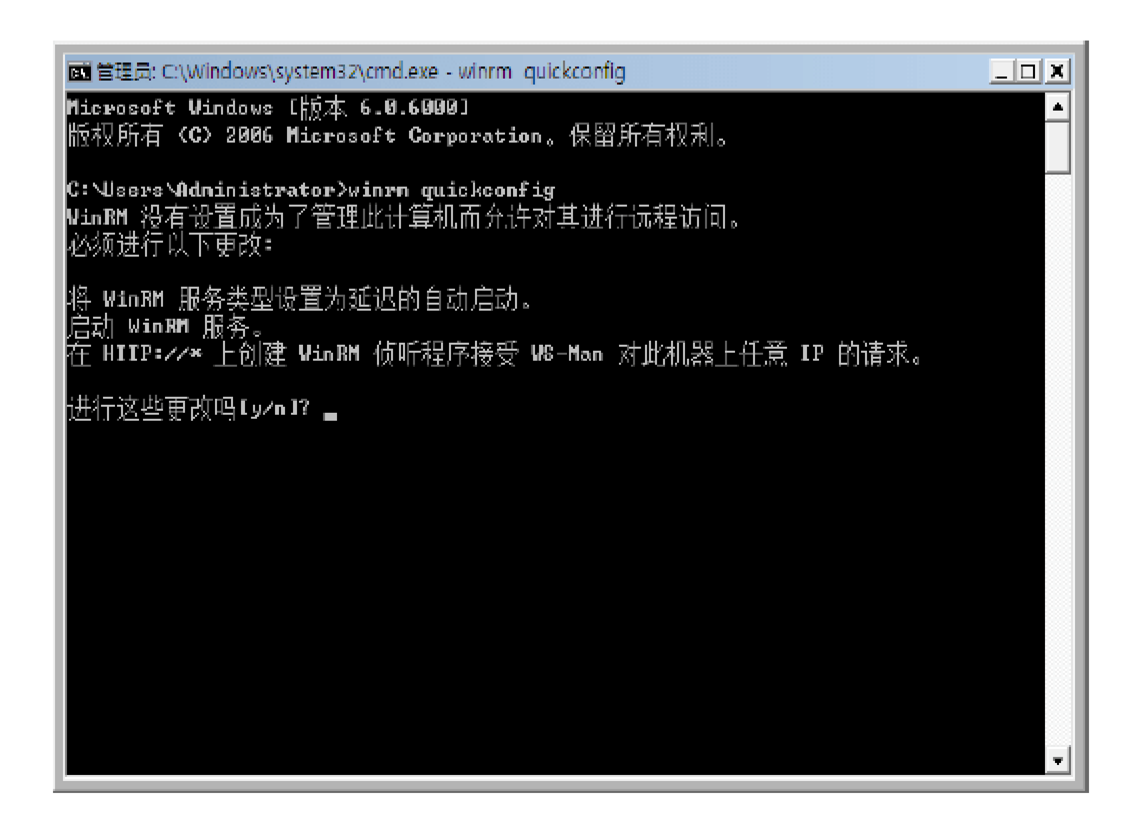


图 18.28 是否允许远程访问

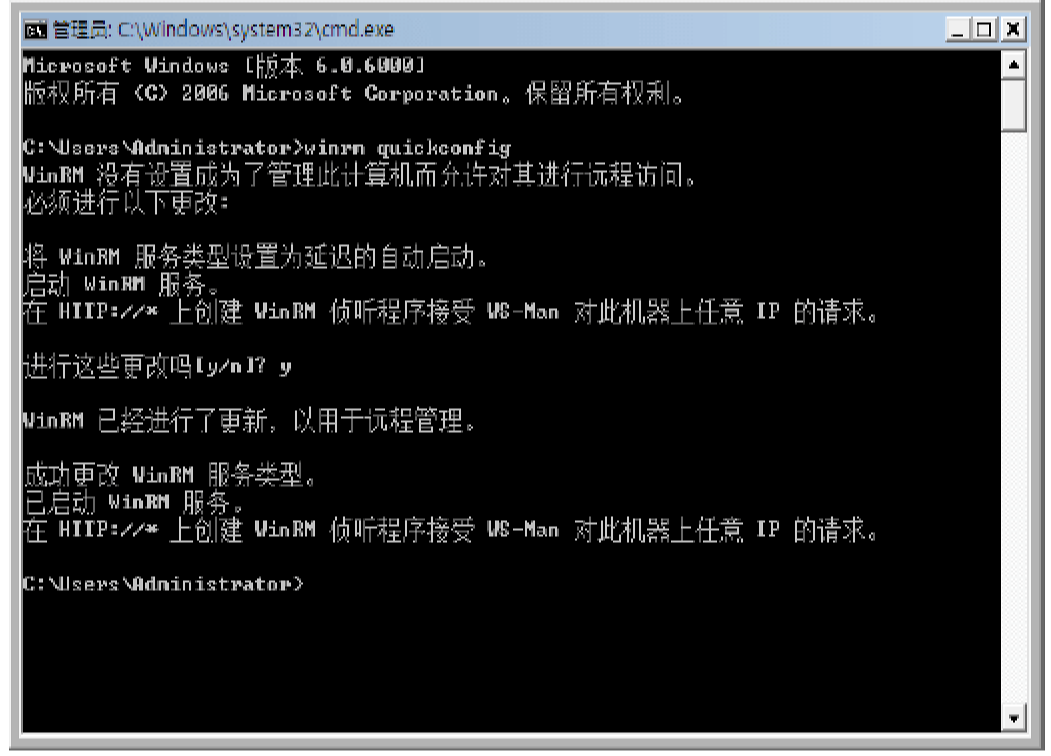


图 18.29 启动 winRM 服务

03 将事件收集服务器的计算机帐户添加到本地计算机的 Administrators 组中。依次单击“开始”→“控制面板”→“管理工具”→“计算机管理”，打开“计算机管理”窗口，展开“系统工具”→“本地用户和组”→“组”项目，双击“Administrators”，打开如图 18.30 所示“Administrators 属性”对话框。

04 单击“添加”按钮，打开“选择用户、计算机或组”对话框。默认情况下，只能向该组中添加用户或组对象。单击“对象类型”按钮，打开“对象类型”对话框，选中“对象类型”列表中的“计算机”，如图 18.31 所示。

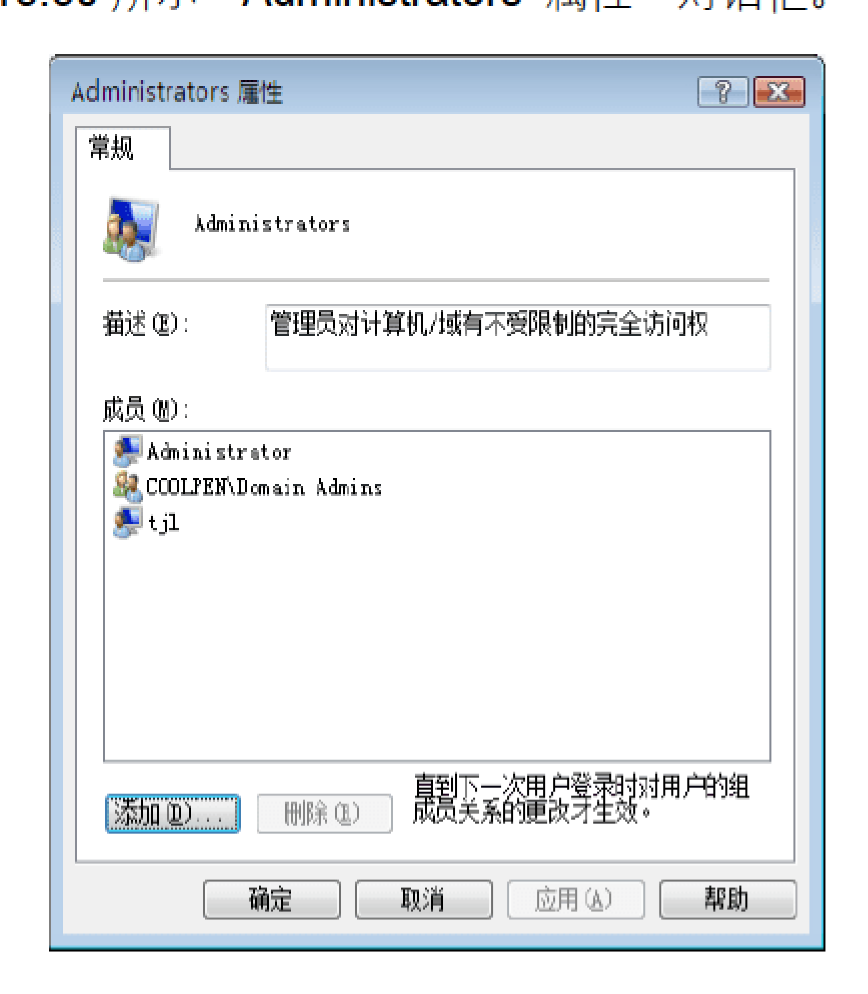


图 18.30 “Administrators 属性”对话框

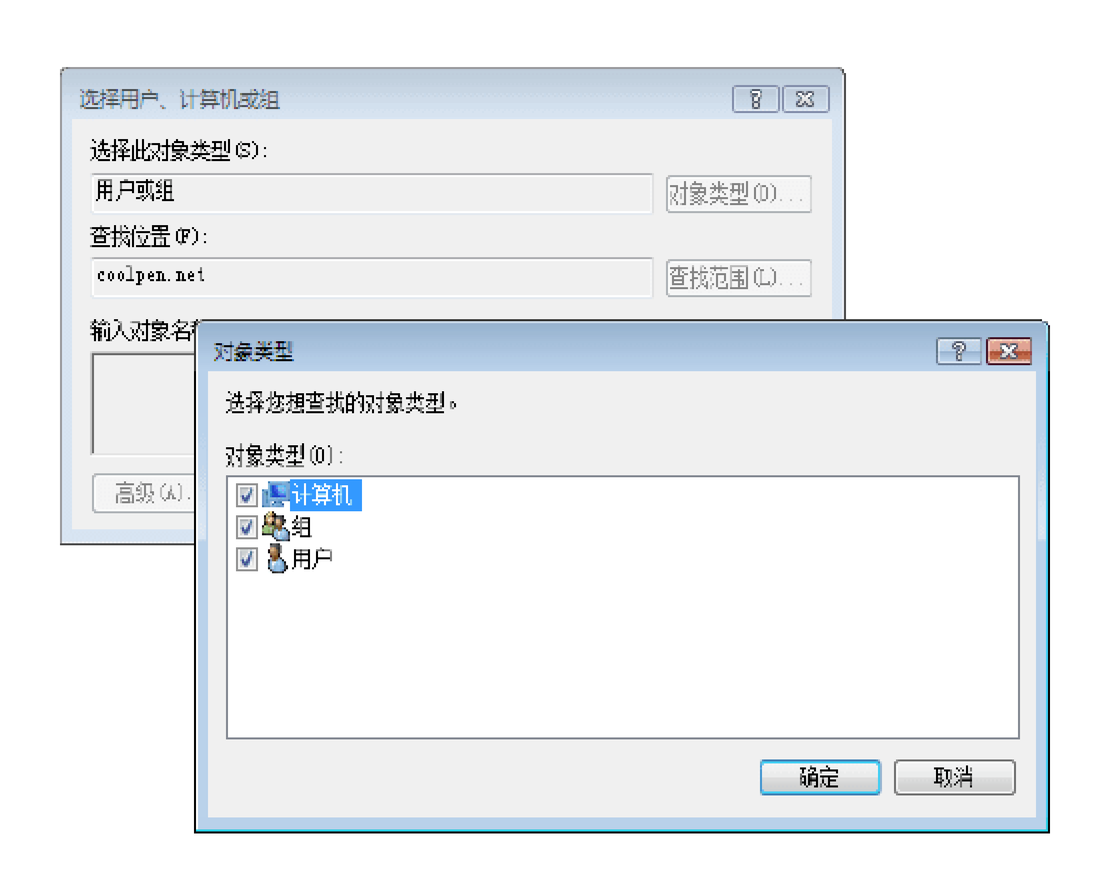


图 18.31 “对象类型”对话框

05 单击“确定”按钮，返回“选择用户、计算机或组”对话框，在“输入对象名称来选择”文本框中，输入事件收集服务器的主机名，如图 18.32 所示。也可以单击“高级”按钮，从指定位置的所有对象中搜索希望添加的服务器。

06 单击“确定”按钮，将其添加至 Administrators 组成员列表中，如图 18.33 所示。





图 18.32　“选择用户、计算机或组”对话框

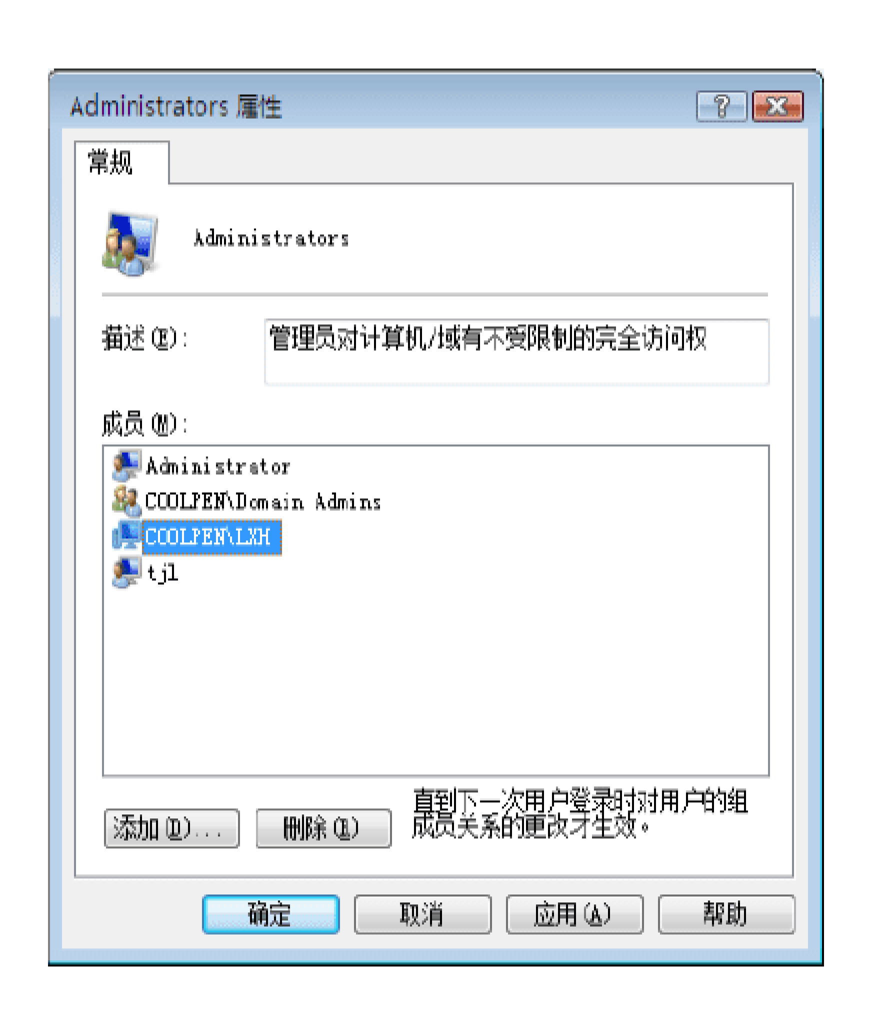


图 18.33　成功添加到成员列表中

提示

重复上述操作，可以配置多台源计算机。

2. 配置收集服务器

如果指定了较多的源计算机，则运行过程中可能产生大量的日志文件，如果源计算机是应用程序服务器，则数据量更大。为确保事件日志的安全，建议采用单独的服务器作为收集服务器，主要配置步骤如下。

01 打开“管理员：命令提示符”窗口，输入如下命令：wecutil qc，按 Enter 键执行，显示如图 18.34 所示结果，提示是否更改服务启动模式。



图 18.34　是否更改服务启动模式

提示

wecutil qc 命令主要用于快速配置事件收集服务器，其中“qc”是“quick-config”的缩写。确认执行该命令后，主要完成如下操作：

- 如果已禁用 ForwardedEvents（转发的事件）通道，则启用该通道；
- 将 Windows 事件收集器服务设置为延迟启动（仅适用于 Windows Vista 和更新的 Windows 系统）；
- 如果 Windows 事件收集器服务未运行，则启动该服务。

02 输入“Y”并按 Enter 键执行，确认执行更改，显示如图 18.35 所示结果，事件收集服务器配置成功。



图 18.35　成功配置事件收集服务器

提示　如果要指定“最小化带宽”或“最小化滞后时间”的事件传递优化，则还必须在收集器计算机上运行 winrm quickconfig 命令。

3. 创建订阅

若要在事件收集服务器上接收来自其他计算机的事件日志，必须创建一个或者多个事件订阅，在源计算机和事件收集服务器上做好上述准备工作之后，即可开始配置事件订阅。

01 在事件收集服务器上打开“事件查看器”窗口，并在导航栏中选择“订阅”，如图 18.36 所示。

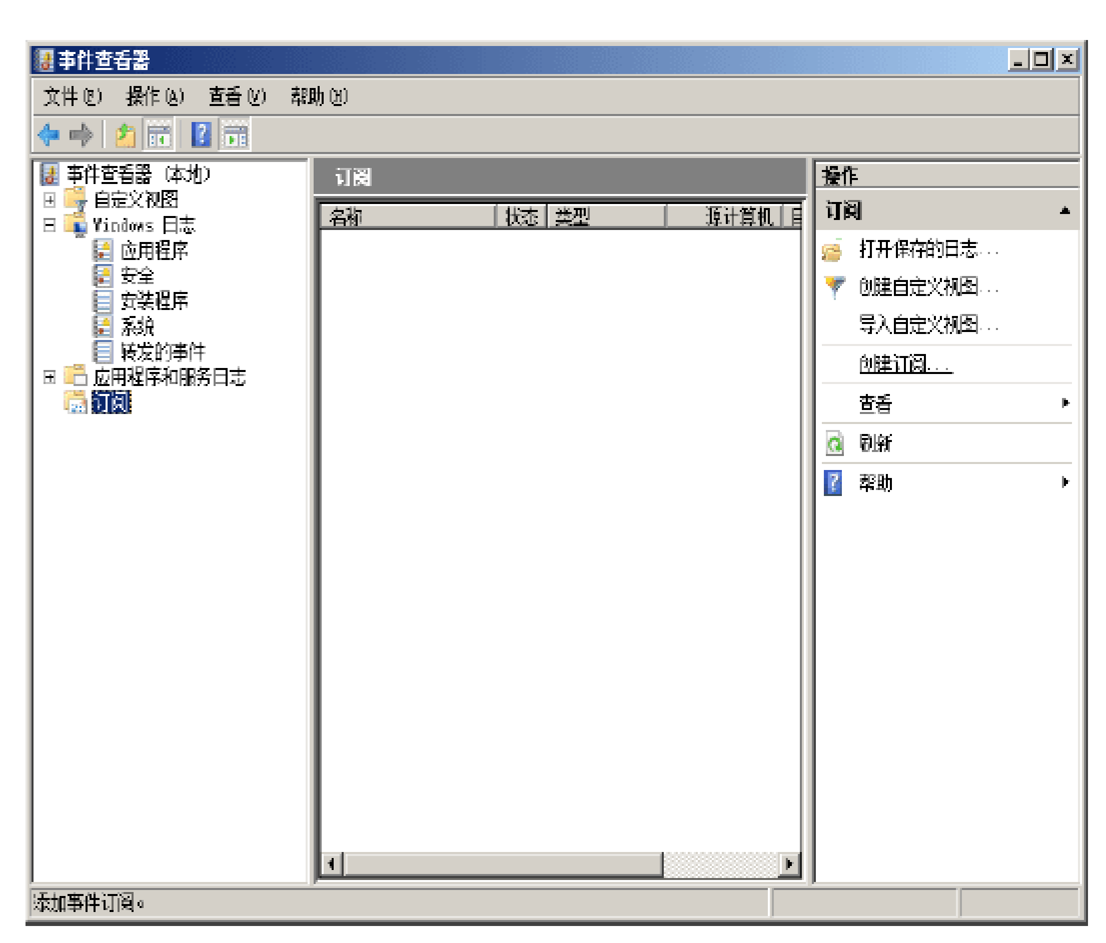


图 18.36　“事件查看器”窗口

提示　默认情况下，Windows Vista 和 Windows Server 2008 系统均未启动事件收集所需的系统服务。在做好事件收集服务器的准备工作之前，选择“订阅”项目时，会提示如图 18.37 所示“事件查看器”对话框。

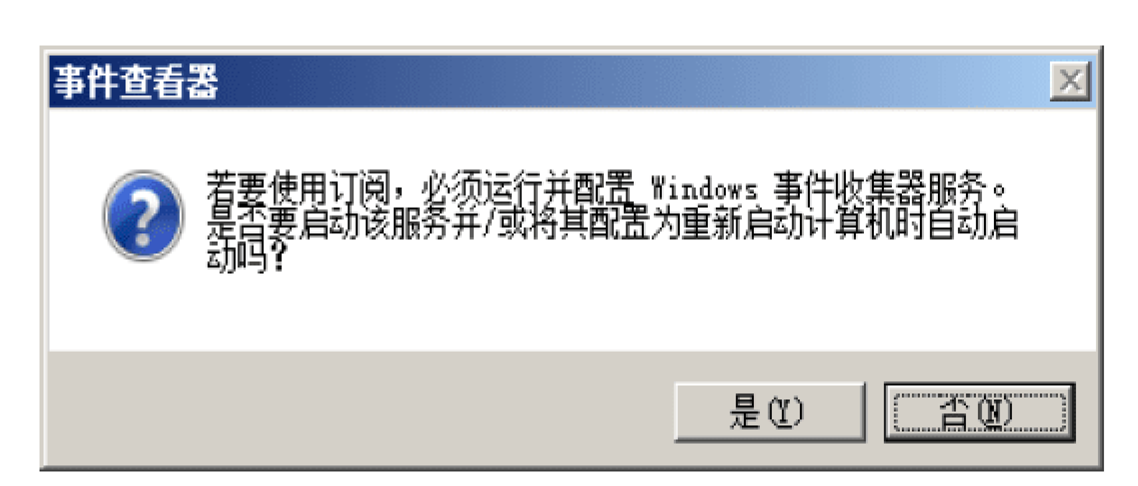


图 18.37　“事件查看器”对话框



02 在事件查看器窗口的“操作”栏中单击“创建订阅”链接，打开如图 18.38 所示“订阅属性”对话框。在“订阅名称”文本框中，输入订阅的名称；在“说明”文本框中可输入相关的说明性文字，以便区分；“目标日志”是用于保存所收集事件的目录，默认目录为“Windows 日志”中的“转发的事件”。

03 在“订阅类型和源计算机”选项区域，选择“收集器已启动”单选按钮，并单击“选择计算机”按钮，打开“计算机”对话框，单击“添加域计算机”按钮，打开如图 18.39 所示“选择计算机”对话框。在“输入要选择的对象名称”文本框中，输入域中源计算机的主机名，可以同时输入多个，彼此之间以分号（;）隔开。也可以单击“高级”按钮，在所有目录对象中查找。

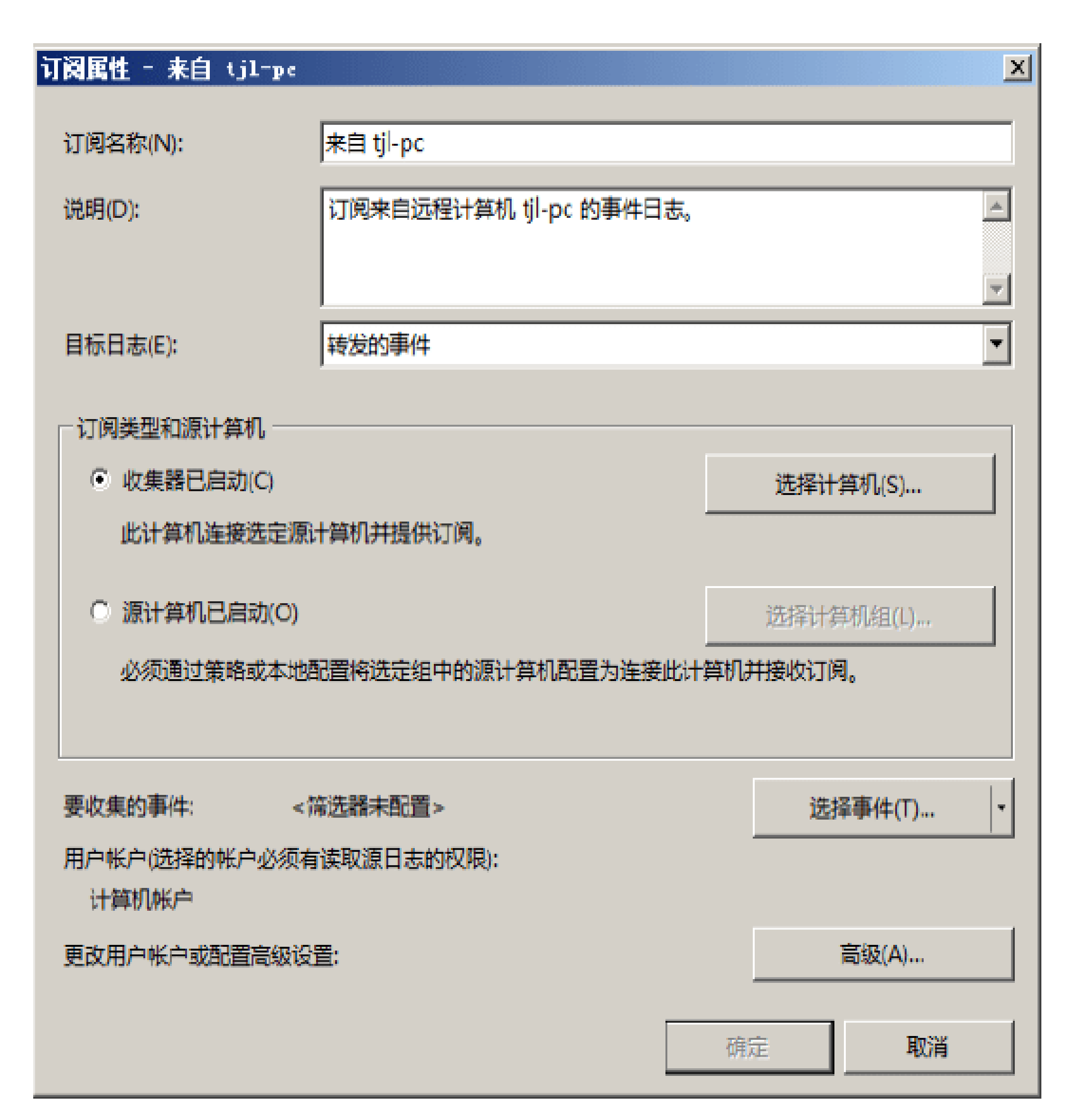


图 18.38　“订阅属性”对话框

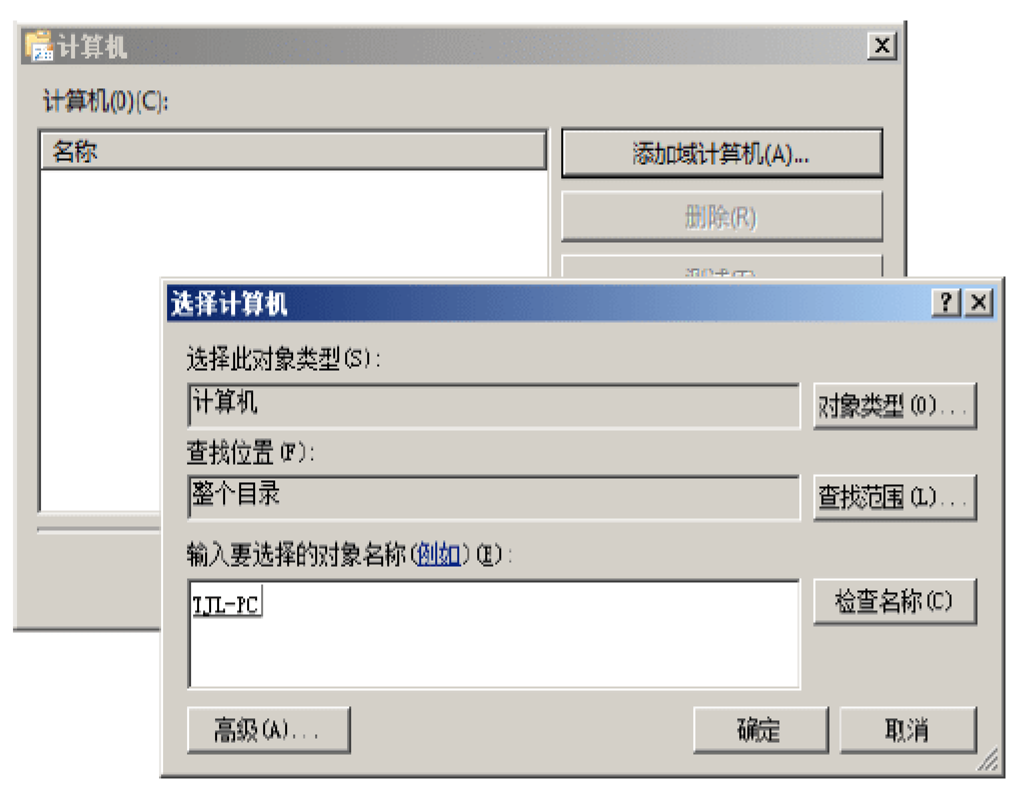


图 18.39　“选择计算机”对话框

04 单击“确定”按钮，将所选计算机添加到“计算机”列表中，如图 18.40 所示。

05 为确保事件收集服务器和所选源计算机之间的连接正常，可以在“计算机”列表中，选中源计算机名称并单击“测试”按钮，如果显示如图 18.41 所示“连接测试成功”的结果，则表示连接正常。

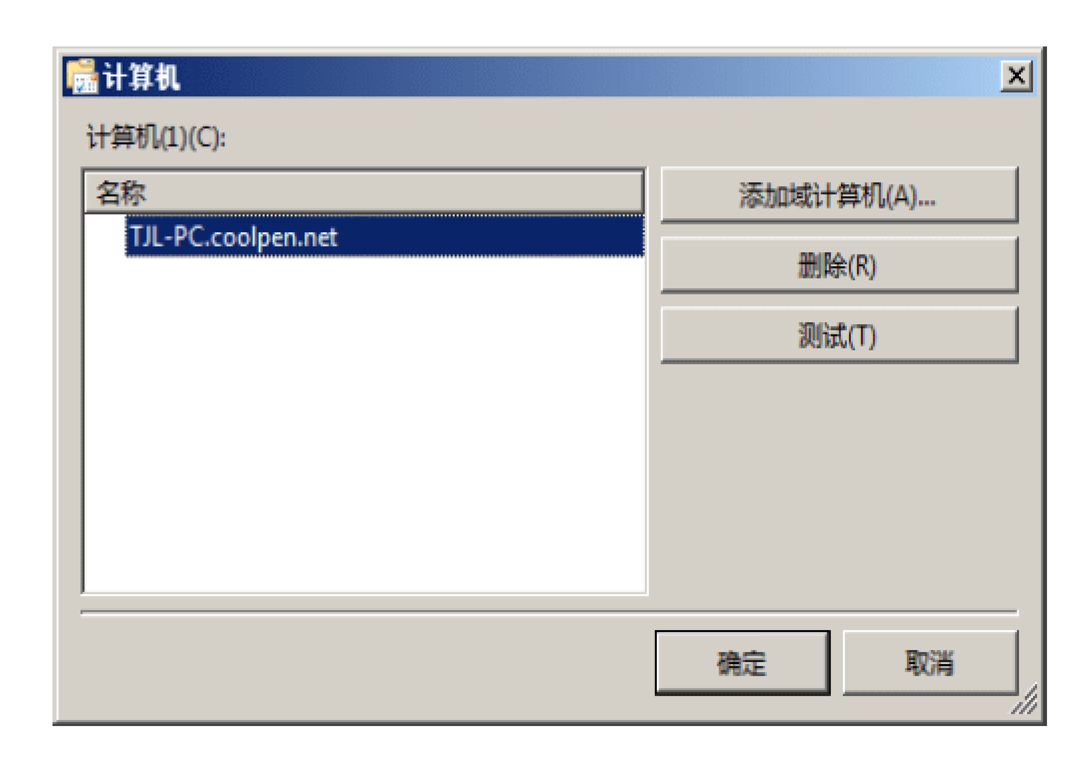


图 18.40　“计算机”对话框



图 18.41　“事件查看器”对话框

06 连续单击“确定”按钮返回至“订阅属性”对话框，单击“选择事件”按钮，打开如图 18.42 所示“查询筛选器”对话框。在“记录时间”下拉列表中选择希望收集的事件产生的时间和日期。在“事件级别”选项区域选择被收集事件的级别，选择“按日志”单选按钮，并在“事件日志”下拉列表中，选择事件类型。需要注意的是，如果选择的事件类型过多，可能需要收集大量的事件，占用大量空间。

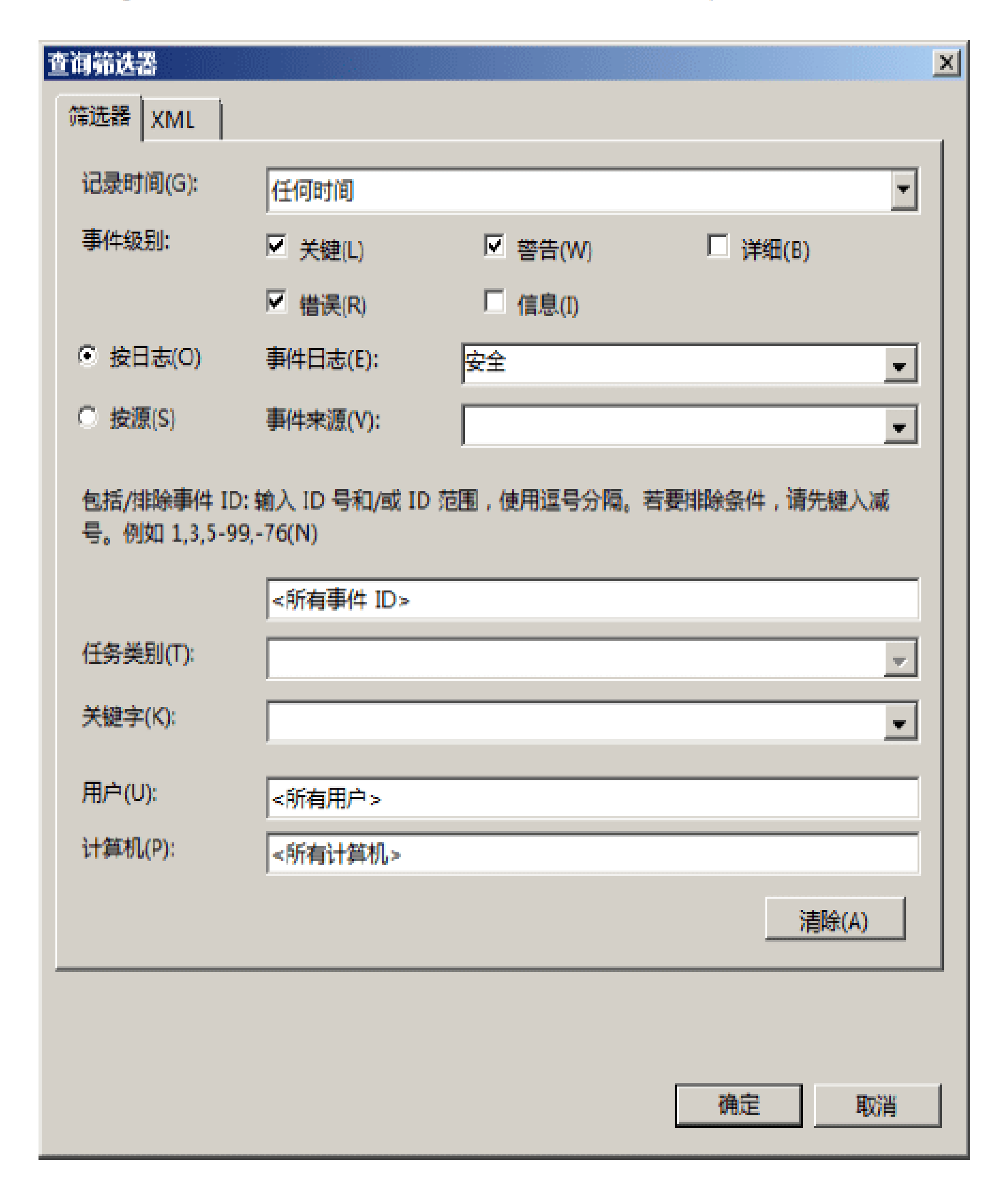


图 18.42 “查询筛选器”对话框

07 单击“确定”按钮，返回“订阅属性”对话框，单击“高级”按钮，打开如图 18.43 所示“高级订阅设置”对话框。由于已经将事件收集服务器的计算机帐户添加到了源计算机的 Administrators 组中，所以选择“计算机帐户”单选按钮即可。

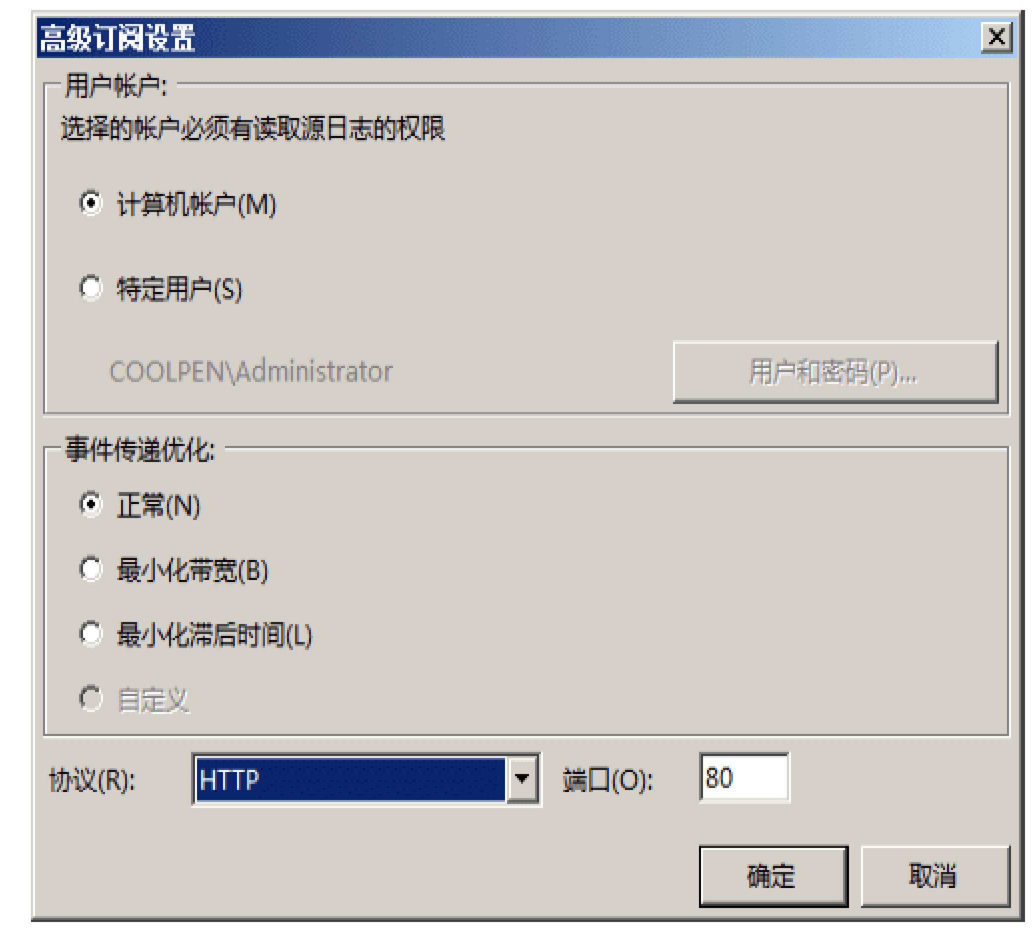


图 18.43 “高级订阅设置”对话框

■ 特定用户。若要指定用于管理收集事件的过程的帐户，则可以选择“特定用户”单选按钮，然后单击“用户和密码”按钮，打开如图 18.44 所示“订阅源的凭据”对话框，输入帐户的用户名和密码即可。



图 18.44 “订阅源的凭据”对话框

■ 事件传递优化。在这里用户可以根据网络连接状况设置适当的优化措施。例如，如果不希望占用过多网络带宽，选择“最小化带宽”单选按钮即可。系统默认为“正常”状态，即不进行任何优化。

■ 协议。系统默认使用 HTTP 协议传出事件，用户也可以在“协议”下拉列表中选择“HTTPS”协议，但是还必须在 Windows 防火墙的“例外”程序中添加“443 端口”。如果使用“正常”(PULL 模式) 传递优化的订阅，则只需在源计算机的防火墙上设置例外；如果使用“最小化带宽”或“最小化滞后时间”(PUSH 模式) 传递优化的订阅，则必须在源计算机和收集器计算机上同时设置例外。

06 连续单击“确定”按钮返回至“订阅属性”对话框，单击“选择事件”按钮，打开如图 18.42 所示“查询筛选器”对话框。在“记录时间”下拉列表中选择希望收集的事件产生的时间和日期。在“事件级别”选项区域选择被收集事件的级别，选择“按日志”单选按钮，并在“事件日志”下拉列表中，选择事件类型。需要注意的是，如果选择的事件类型过多，可能需要收集大量的事件，占用大量空间。

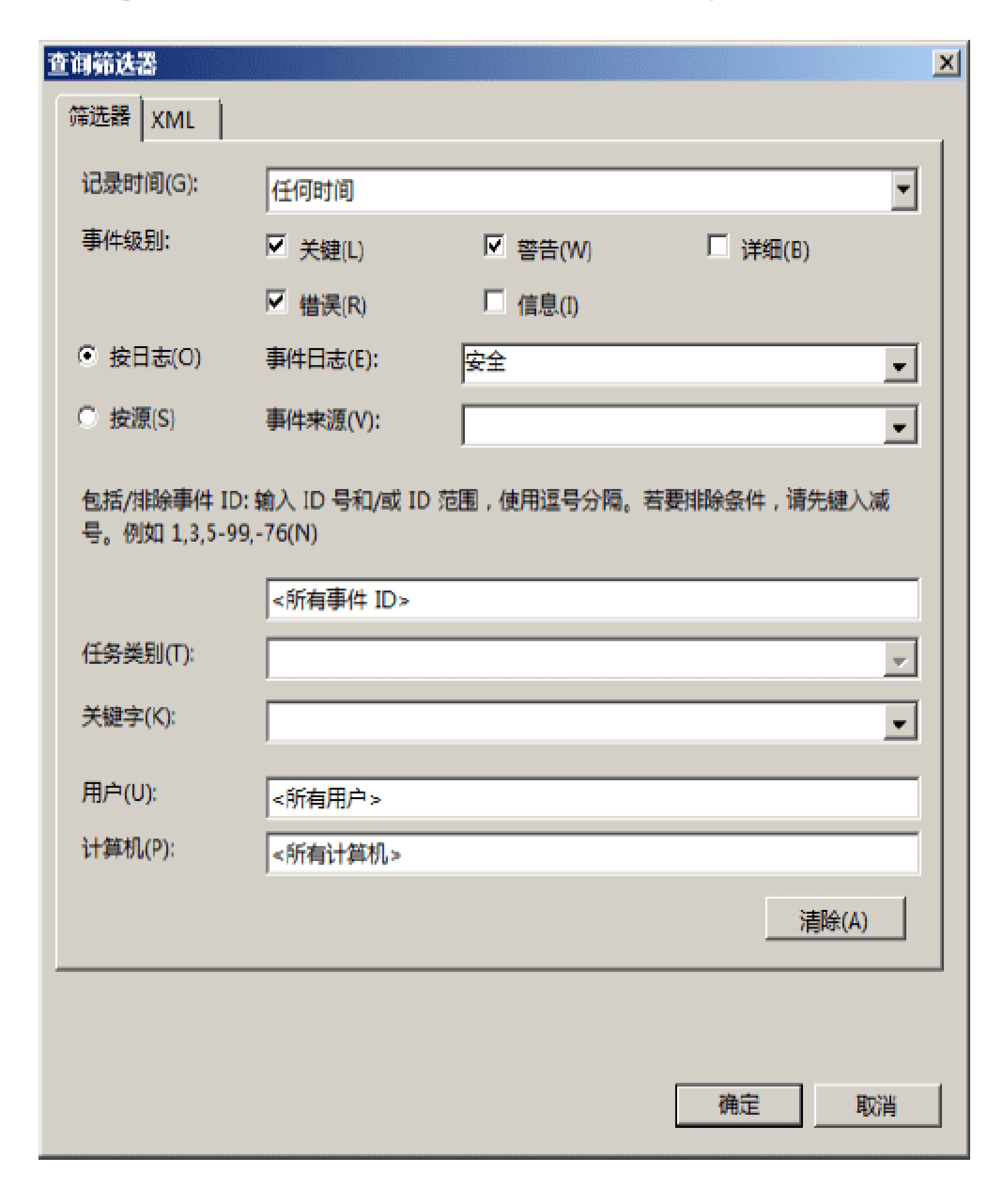


图 18.42 “查询筛选器”对话框

07 单击“确定”按钮，返回“订阅属性”对话框，单击“高级”按钮，打开如图 18.43 所示“高级订阅设置”对话框。由于已经将事件收集服务器的计算机帐户添加到了源计算机的 Administrators 组中，所以选择“计算机帐户”单选按钮即可。

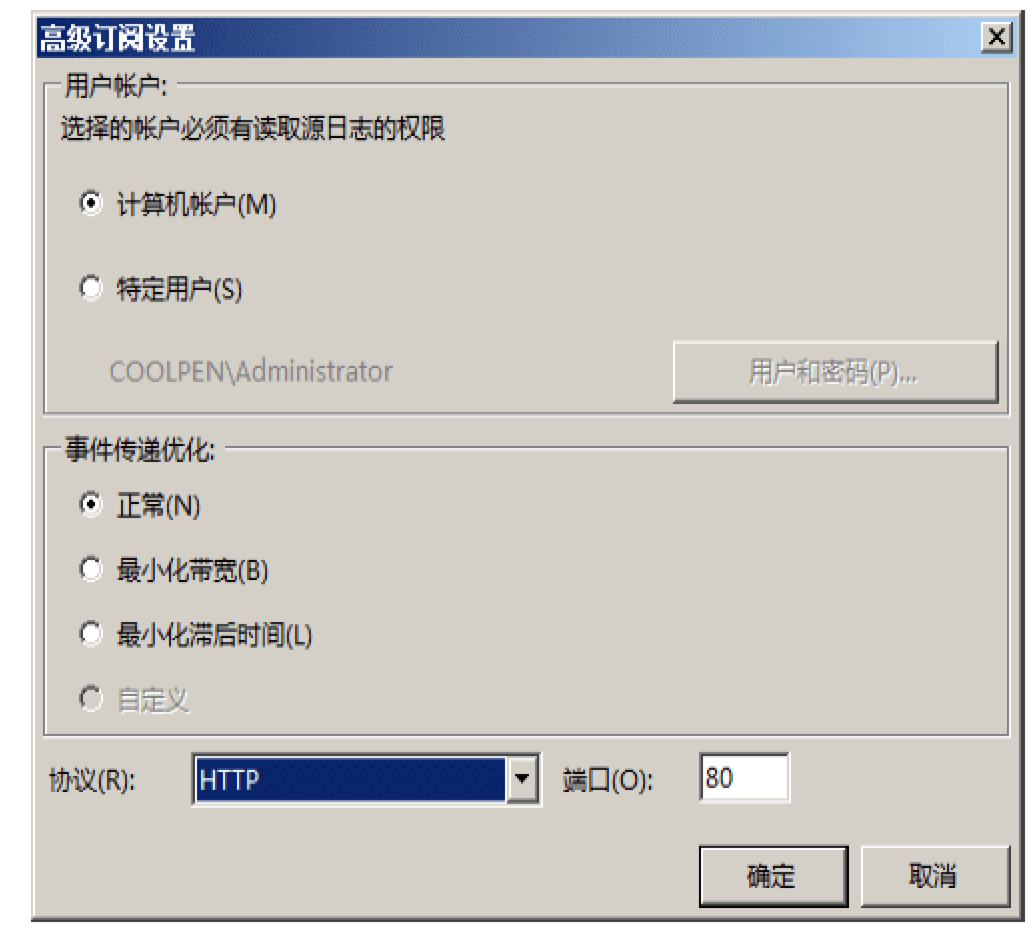


图 18.43 “高级订阅设置”对话框

- 特定用户。若要指定用于管理收集事件的过程的帐户，则可以选择“特定用户”单选按钮，然后单击“用户和密码”按钮，打开如图 18.44 所示“订阅源的凭据”对话框，输入帐户的用户名和密码即可。



图 18.44 “订阅源的凭据”对话框

- 事件传递优化。在这里用户可以根据网络连接状况设置适当的优化措施。例如，如果不希望占用过多网络带宽，选择“最小化带宽”单选按钮即可。系统默认为“正常”状态，即不进行任何优化。
- 协议。系统默认使用 HTTP 协议传出事件，用户也可以在“协议”下拉列表中选择“HTTPS”协议，但是还必须在 Windows 防火墙的“例外”程序中添加“443 端口”。如果使用“正常”(PULL 模式) 传递优化的订阅，则只需在源计算机的防火墙上设置例外；如果使用“最小化带宽”或“最小化滞后时间”(PUSH 模式) 传递优化的订阅，则必须在源计算机和收集器计算机上同时设置例外。

06 连续单击“确定”按钮返回至“订阅属性”对话框，单击“选择事件”按钮，打开如图 18.42 所示“查询筛选器”对话框。在“记录时间”下拉列表中选择希望收集的事件产生的时间和日期。在“事件级别”选项区域选择被收集事件的级别，选择“按日志”单选按钮，并在“事件日志”下拉列表中，选择事件类型。需要注意的是，如果选择的事件类型过多，可能需要收集大量的事件，占用大量空间。

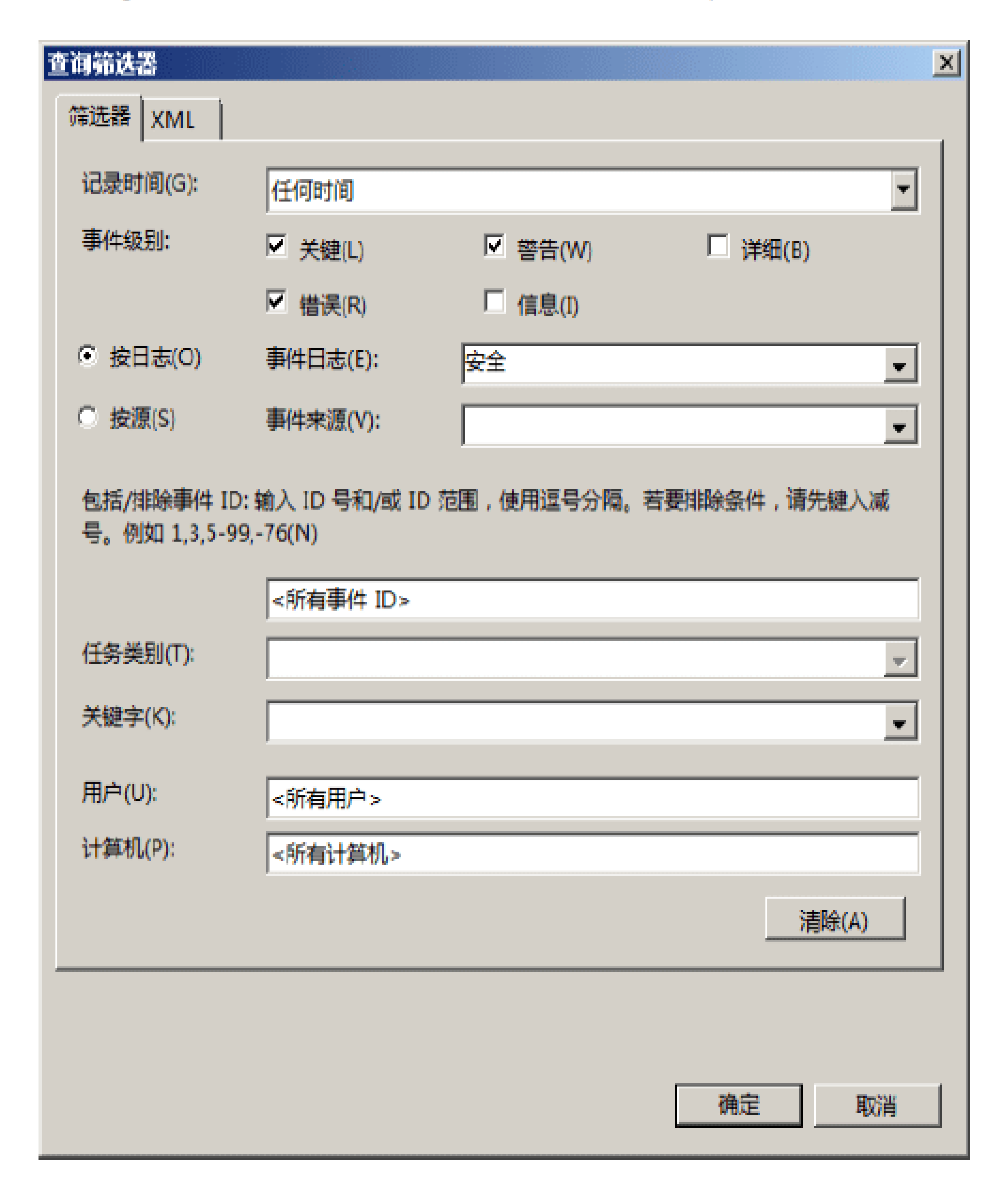


图 18.42 “查询筛选器”对话框

07 单击“确定”按钮，返回“订阅属性”对话框，单击“高级”按钮，打开如图 18.43 所示“高级订阅设置”对话框。由于已经将事件收集服务器的计算机帐户添加到了源计算机的 Administrators 组中，所以选择“计算机帐户”单选按钮即可。

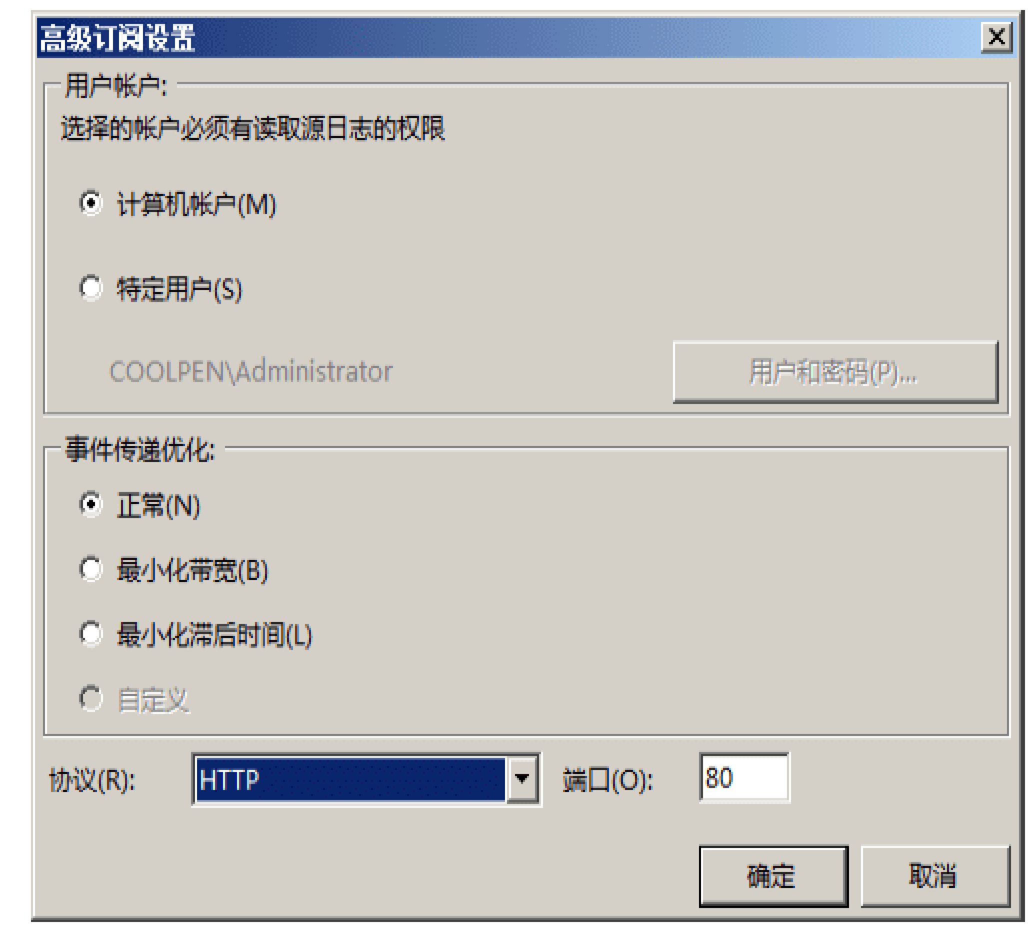


图 18.43 “高级订阅设置”对话框

- 特定用户。若要指定用于管理收集事件的过程的帐户，则可以选择“特定用户”单选按钮，然后单击“用户和密码”按钮，打开如图 18.44 所示“订阅源的凭据”对话框，输入帐户的用户名和密码即可。



图 18.44 “订阅源的凭据”对话框

- 事件传递优化。在这里用户可以根据网络连接状况设置适当的优化措施。例如，如果不希望占用过多网络带宽，选择“最小化带宽”单选按钮即可。系统默认为“正常”状态，即不进行任何优化。
- 协议。系统默认使用 HTTP 协议传出事件，用户也可以在“协议”下拉列表中选择“HTTPS”协议，但是还必须在 Windows 防火墙的“例外”程序中添加“443 端口”。如果使用“正常”（PULL 模式）传递优化的订阅，则只需在源计算机的防火墙上设置例外；如果使用“最小化带宽”或“最小化滞后时间”（PUSH 模式）传递优化的订阅，则必须在源计算机和收集器计算机上同时设置例外。

06 连续单击“确定”按钮返回至“订阅属性”对话框，单击“选择事件”按钮，打开如图 18.42 所示“查询筛选器”对话框。在“记录时间”下拉列表中选择希望收集的事件产生的时间和日期。在“事件级别”选项区域选择被收集事件的级别，选择“按日志”单选按钮，并在“事件日志”下拉列表中，选择事件类型。需要注意的是，如果选择的事件类型过多，可能需要收集大量的事件，占用大量空间。

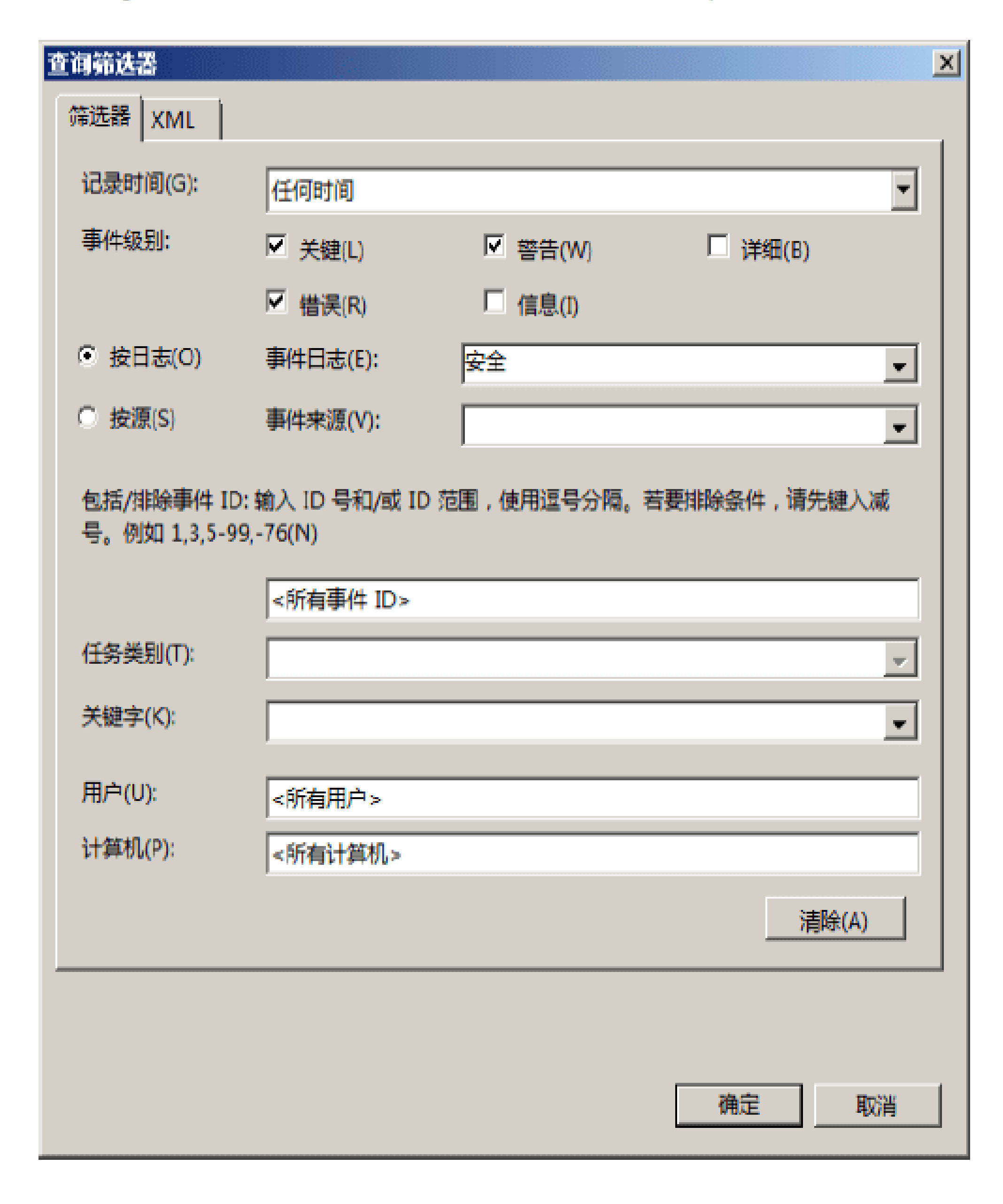


图 18.42 “查询筛选器”对话框

07 单击“确定”按钮，返回“订阅属性”对话框，单击“高级”按钮，打开如图 18.43 所示“高级订阅设置”对话框。由于已经将事件收集服务器的计算机帐户添加到了源计算机的 Administrators 组中，所以选择“计算机帐户”单选按钮即可。

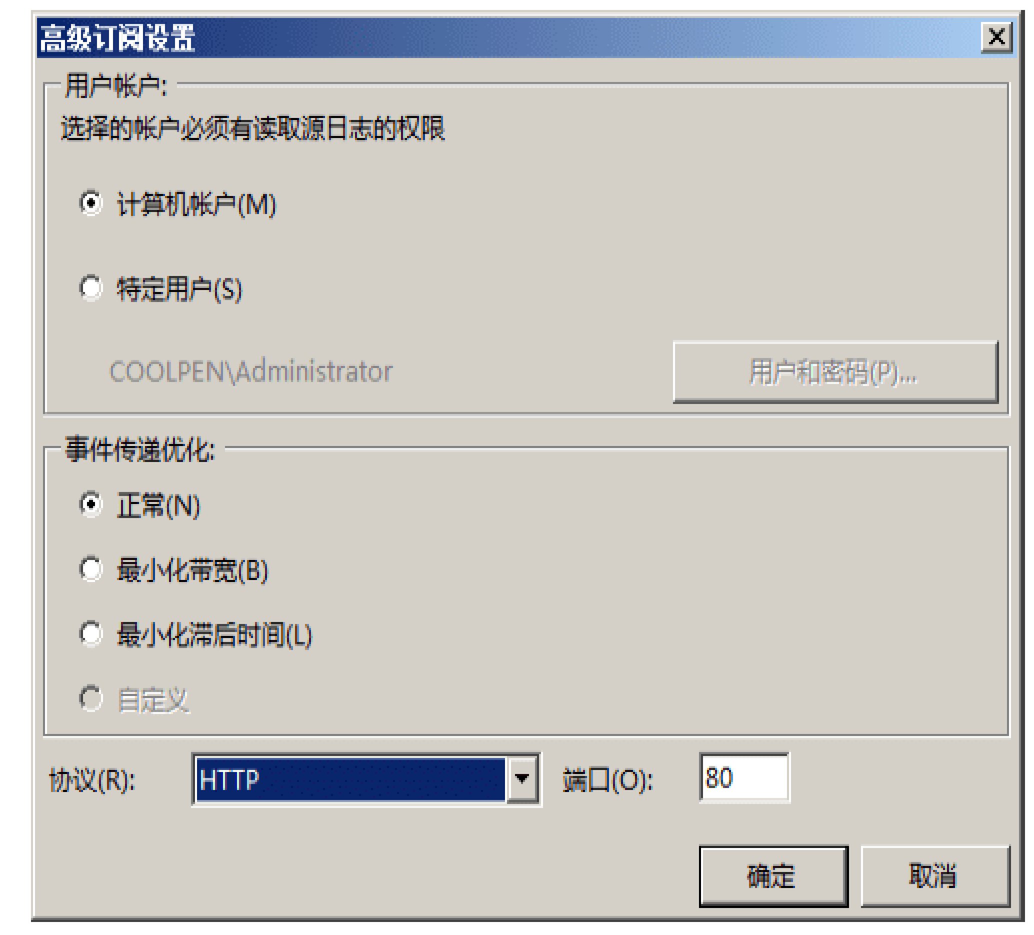


图 18.43 “高级订阅设置”对话框

■ 特定用户。若要指定用于管理收集事件的过程的帐户，则可以选择“特定用户”单选按钮，然后单击“用户和密码”按钮，打开如图 18.44 所示“订阅源的凭据”对话框，输入帐户的用户名和密码即可。

■ 事件传递优化。在这里用户可以根据网络连接状况设置适当的优化措施。例如，如果不希望占用过多网络带宽，选择“最小化带宽”单选按钮即可。系统默认为“正常”状态，即不进行任何优化。



图 18.44 “订阅源的凭据”对话框

■ 协议。系统默认使用 HTTP 协议传出事件，用户也可以在“协议”下拉列表中选择“HTTPS”协议，但是还必须在 Windows 防火墙的“例外”程序中添加“443 端口”。如果使用“正常”(PULL 模式) 传递优化的订阅，则只需在源计算机的防火墙上设置例外；如果使用“最小化带宽”或“最小化滞后时间”(PUSH 模式) 传递优化的订阅，则必须在源计算机和收集器计算机上同时设置例外。

06 连续单击“确定”按钮返回至“订阅属性”对话框，单击“选择事件”按钮，打开如图 18.42 所示“查询筛选器”对话框。在“记录时间”下拉列表中选择希望收集的事件产生的时间和日期。在“事件级别”选项区域选择被收集事件的级别，选择“按日志”单选按钮，并在“事件日志”下拉列表中，选择事件类型。需要注意的是，如果选择的事件类型过多，可能需要收集大量的事件，占用大量空间。

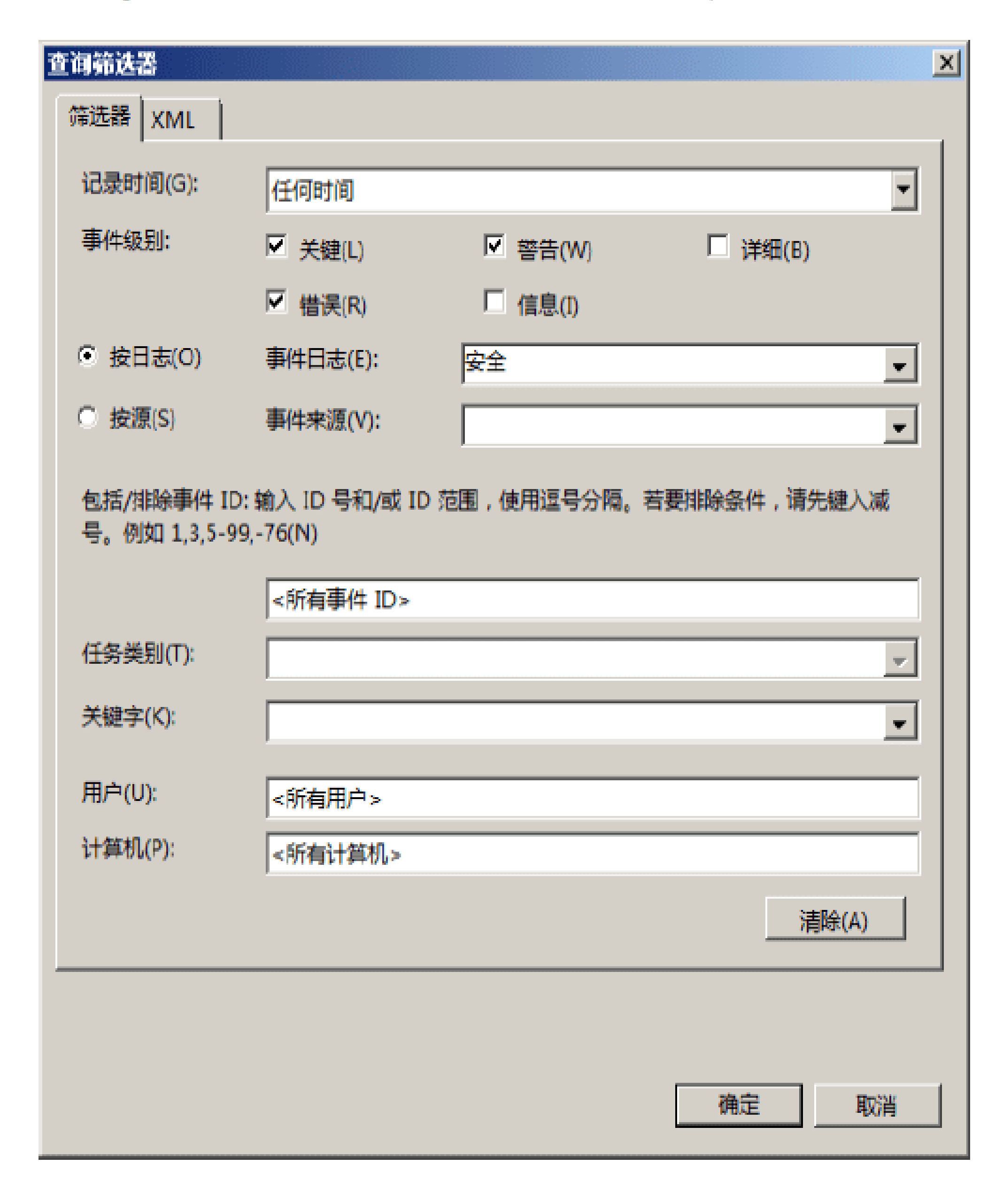


图 18.42 “查询筛选器”对话框

07 单击“确定”按钮，返回“订阅属性”对话框，单击“高级”按钮，打开如图 18.43 所示“高级订阅设置”对话框。由于已经将事件收集服务器的计算机帐户添加到了源计算机的 Administrators 组中，所以选择“计算机帐户”单选按钮即可。

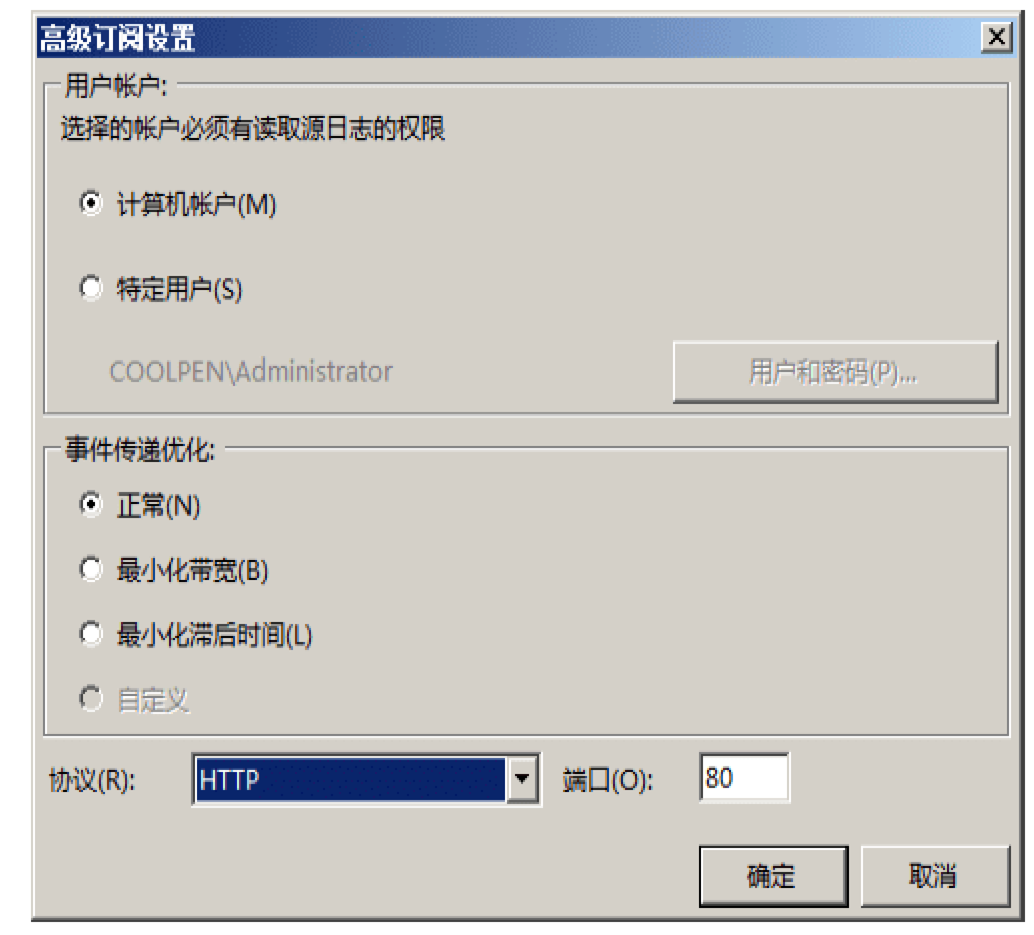


图 18.43 “高级订阅设置”对话框

- 特定用户。若要指定用于管理收集事件的过程的帐户，则可以选择“特定用户”单选按钮，然后单击“用户和密码”按钮，打开如图 18.44 所示“订阅源的凭据”对话框，输入帐户的用户名和密码即可。



图 18.44 “订阅源的凭据”对话框

- 事件传递优化。在这里用户可以根据网络连接状况设置适当的优化措施。例如，如果不希望占用过多网络带宽，选择“最小化带宽”单选按钮即可。系统默认为“正常”状态，即不进行任何优化。
- 协议。系统默认使用 HTTP 协议传出事件，用户也可以在“协议”下拉列表中选择“HTTPS”协议，但是还必须在 Windows 防火墙的“例外”程序中添加“443 端口”。如果使用“正常”(PULL 模式）传递优化的订阅，则只需在源计算机的防火墙上设置例外；如果使用“最小化带宽”或“最小化滞后时间”(PUSH 模式）传递优化的订阅，则必须在源计算机和收集器计算机上同时设置例外。

06 连续单击“确定”按钮返回至“订阅属性”对话框，单击“选择事件”按钮，打开如图 18.42 所示“查询筛选器”对话框。在“记录时间”下拉列表中选择希望收集的事件产生的时间和日期。在“事件级别”选项区域选择被收集事件的级别，选择“按日志”单选按钮，并在“事件日志”下拉列表中，选择事件类型。需要注意的是，如果选择的事件类型过多，可能需要收集大量的事件，占用大量空间。

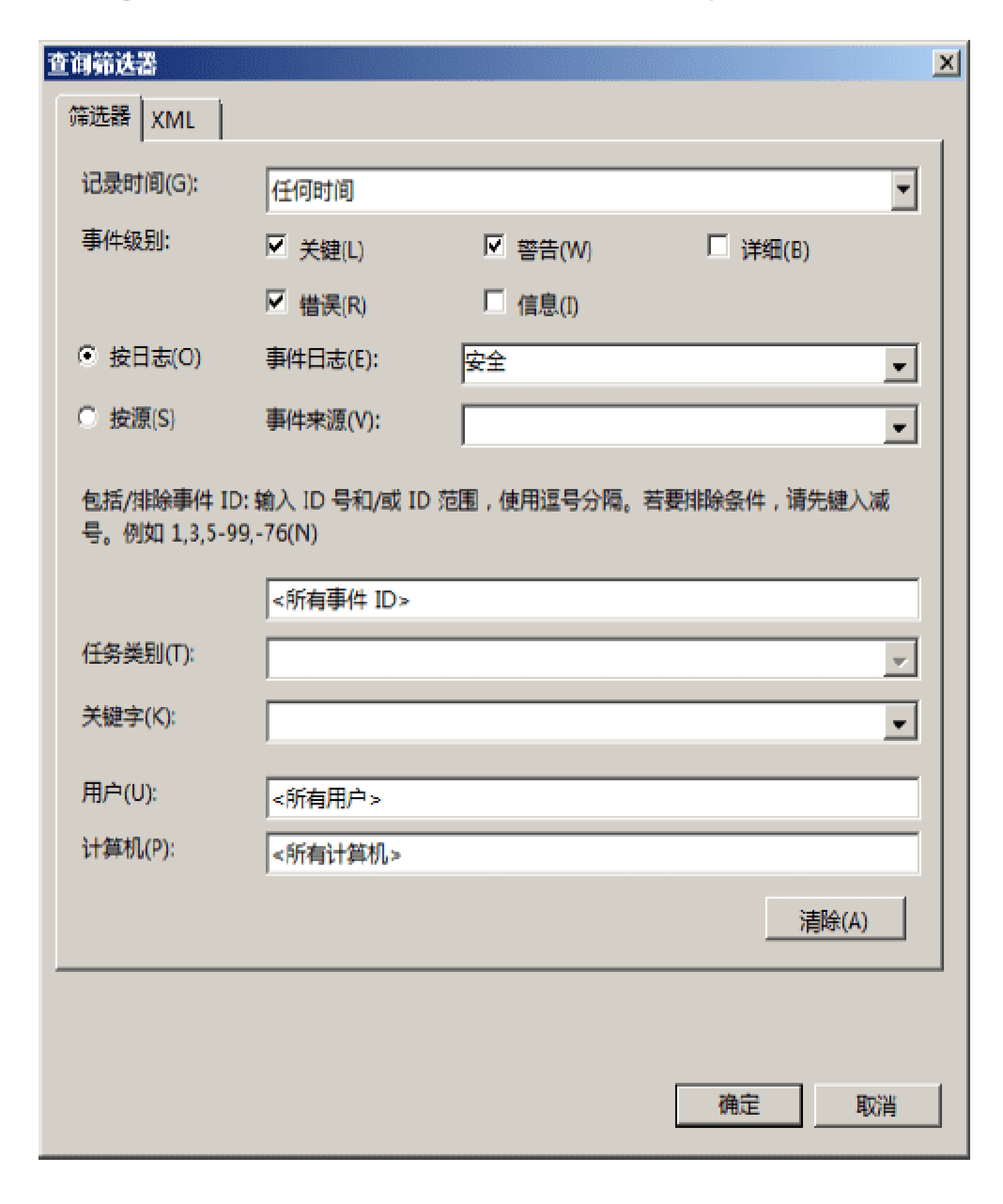


图 18.42 “查询筛选器”对话框

07 单击“确定”按钮，返回“订阅属性”对话框，单击“高级”按钮，打开如图 18.43 所示“高级订阅设置”对话框。由于已经将事件收集服务器的计算机帐户添加到了源计算机的 Administrators 组中，所以选择“计算机帐户”单选按钮即可。

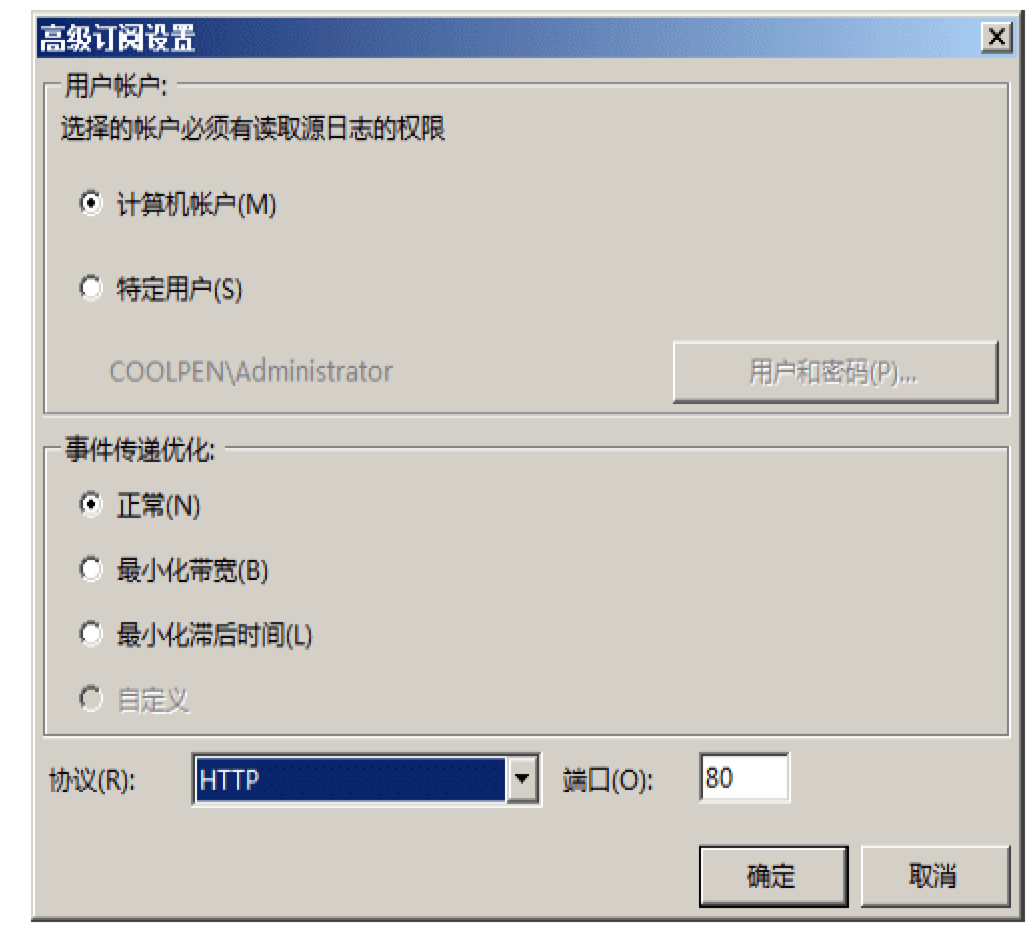


图 18.43 “高级订阅设置”对话框

- 特定用户。若要指定用于管理收集事件的过程的帐户，则可以选择“特定用户”单选按钮，然后单击“用户和密码”按钮，打开如图 18.44 所示“订阅源的凭据”对话框，输入帐户的用户名和密码即可。



图 18.44 “订阅源的凭据”对话框

- 事件传递优化。在这里用户可以根据网络连接状况设置适当的优化措施。例如，如果不希望占用过多网络带宽，选择“最小化带宽”单选按钮即可。系统默认为“正常”状态，即不进行任何优化。
- 协议。系统默认使用 HTTP 协议传出事件，用户也可以在“协议”下拉列表中选择“HTTPS”协议，但是还必须在 Windows 防火墙的“例外”程序中添加“443 端口”。如果使用“正常”(PULL 模式) 传递优化的订阅，则只需在源计算机的防火墙上设置例外；如果使用“最小化带宽”或“最小化滞后时间”(PUSH 模式) 传递优化的订阅，则必须在源计算机和收集器计算机上同时设置例外。

06 连续单击“确定”按钮返回至“订阅属性”对话框，单击“选择事件”按钮，打开如图 18.42 所示“查询筛选器”对话框。在“记录时间”下拉列表中选择希望收集的事件产生的时间和日期。在“事件级别”选项区域选择被收集事件的级别，选择“按日志”单选按钮，并在“事件日志”下拉列表中，选择事件类型。需要注意的是，如果选择的事件类型过多，可能需要收集大量的事件，占用大量空间。

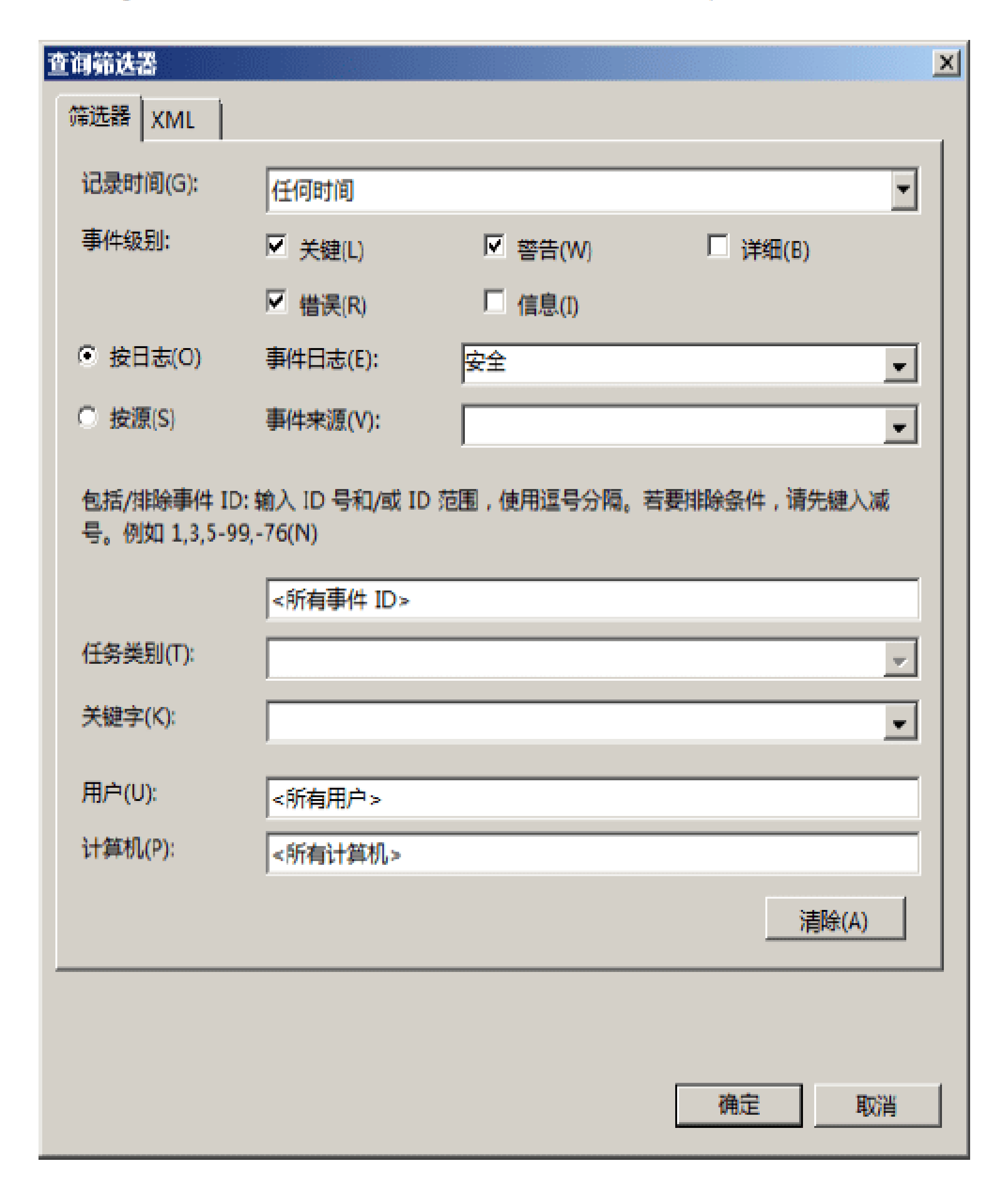


图 18.42 “查询筛选器”对话框

07 单击“确定”按钮，返回“订阅属性”对话框，单击“高级”按钮，打开如图 18.43 所示“高级订阅设置”对话框。由于已经将事件收集服务器的计算机帐户添加到了源计算机的 Administrators 组中，所以选择“计算机帐户”单选按钮即可。

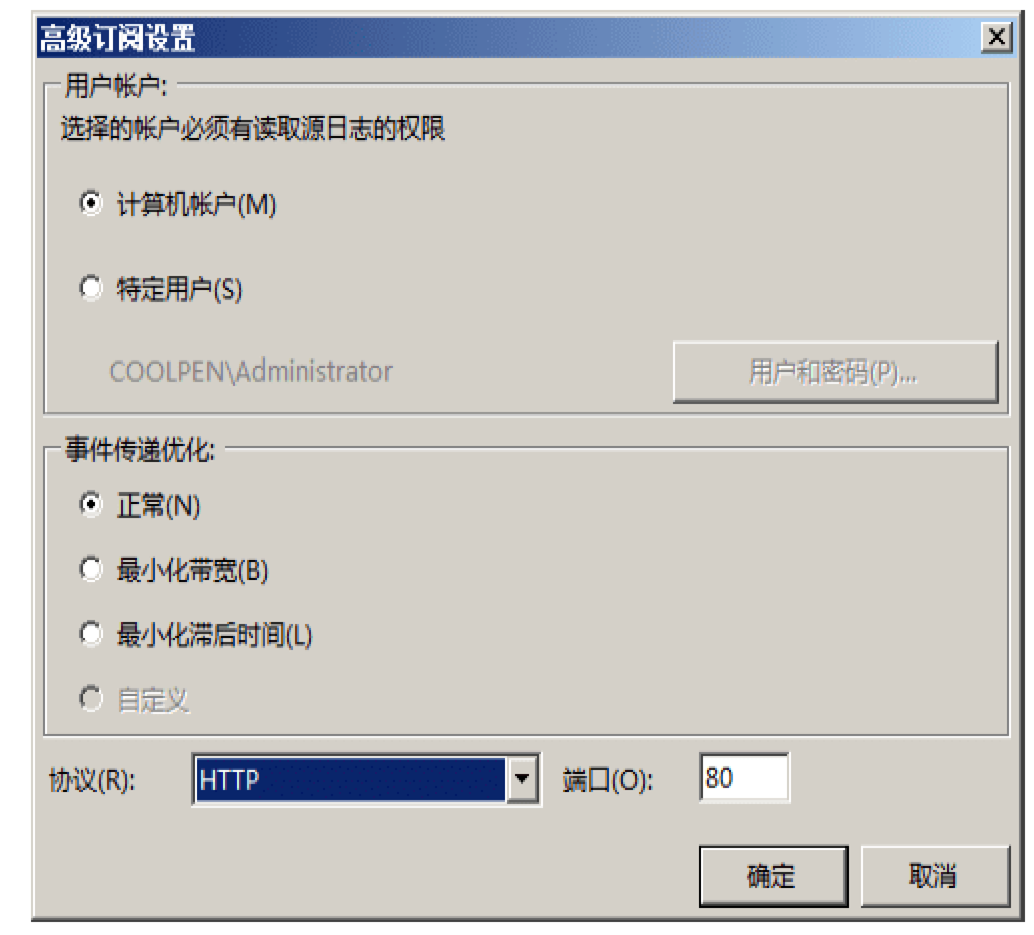


图 18.43 “高级订阅设置”对话框

- 特定用户。若要指定用于管理收集事件的过程的帐户，则可以选择“特定用户”单选按钮，然后单击“用户和密码”按钮，打开如图 18.44 所示“订阅源的凭据”对话框，输入帐户的用户名和密码即可。



图 18.44 “订阅源的凭据”对话框

- 事件传递优化。在这里用户可以根据网络连接状况设置适当的优化措施。例如，如果不希望占用过多网络带宽，选择“最小化带宽”单选按钮即可。系统默认为“正常”状态，即不进行任何优化。
- 协议。系统默认使用 HTTP 协议传出事件，用户也可以在“协议”下拉列表中选择“HTTPS”协议，但是还必须在 Windows 防火墙的“例外”程序中添加“443 端口”。如果使用“正常”(PULL 模式) 传递优化的订阅，则只需在源计算机的防火墙上设置例外；如果使用“最小化带宽”或“最小化滞后时间”(PUSH 模式) 传递优化的订阅，则必须在源计算机和收集器计算机上同时设置例外。

06 连续单击“确定”按钮返回至“订阅属性”对话框，单击“选择事件”按钮，打开如图 18.42 所示“查询筛选器”对话框。在“记录时间”下拉列表中选择希望收集的事件产生的时间和日期。在“事件级别”选项区域选择被收集事件的级别，选择“按日志”单选按钮，并在“事件日志”下拉列表中，选择事件类型。需要注意的是，如果选择的事件类型过多，可能需要收集大量的事件，占用大量空间。

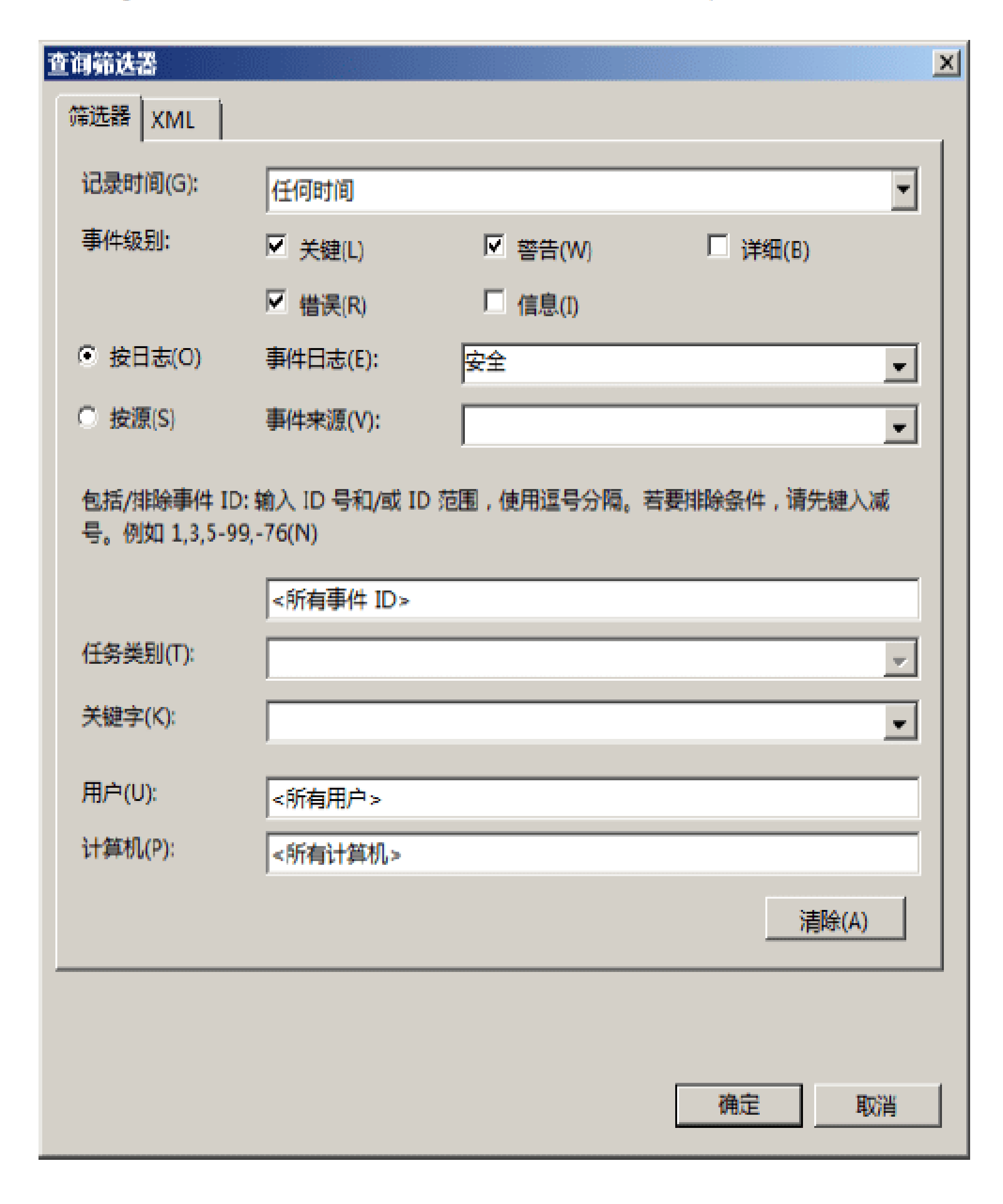


图 18.42 “查询筛选器”对话框

07 单击“确定”按钮，返回“订阅属性”对话框，单击“高级”按钮，打开如图 18.43 所示“高级订阅设置”对话框。由于已经将事件收集服务器的计算机帐户添加到了源计算机的 Administrators 组中，所以选择“计算机帐户”单选按钮即可。

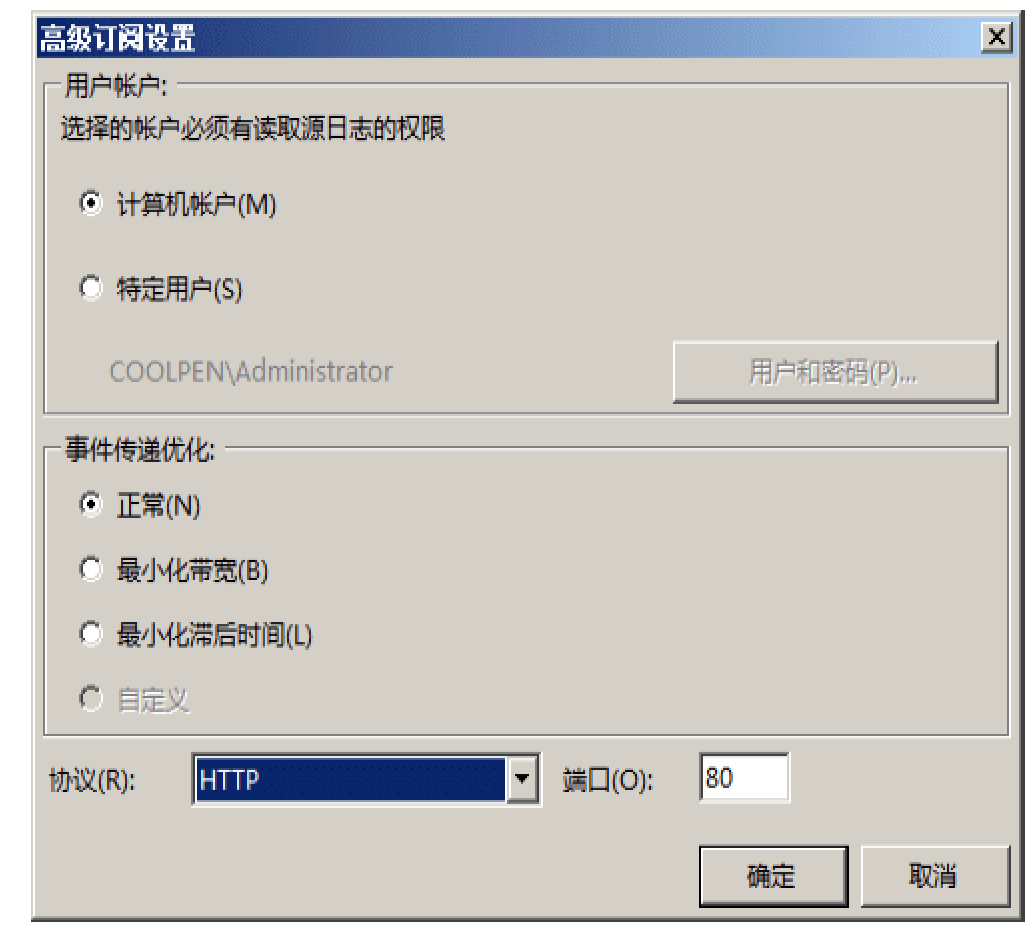


图 18.43 “高级订阅设置”对话框

- 特定用户。若要指定用于管理收集事件的过程的帐户，则可以选择“特定用户”单选按钮，然后单击“用户和密码”按钮，打开如图 18.44 所示“订阅源的凭据”对话框，输入帐户的用户名和密码即可。



图 18.44 “订阅源的凭据”对话框

- 事件传递优化。在这里用户可以根据网络连接状况设置适当的优化措施。例如，如果不希望占用过多网络带宽，选择“最小化带宽”单选按钮即可。系统默认为“正常”状态，即不进行任何优化。
- 协议。系统默认使用 HTTP 协议传出事件，用户也可以在“协议”下拉列表中选择“HTTPS”协议，但是还必须在 Windows 防火墙的“例外”程序中添加“443 端口”。如果使用“正常”（PULL 模式）传递优化的订阅，则只需在源计算机的防火墙上设置例外；如果使用“最小化带宽”或“最小化滞后时间”（PUSH 模式）传递优化的订阅，则必须在源计算机和收集器计算机上同时设置例外。

06 连续单击“确定”按钮返回至“订阅属性”对话框，单击“选择事件”按钮，打开如图 18.42 所示“查询筛选器”对话框。在“记录时间”下拉列表中选择希望收集的事件产生的时间和日期。在“事件级别”选项区域选择被收集事件的级别，选择“按日志”单选按钮，并在“事件日志”下拉列表中，选择事件类型。需要注意的是，如果选择的事件类型过多，可能需要收集大量的事件，占用大量空间。

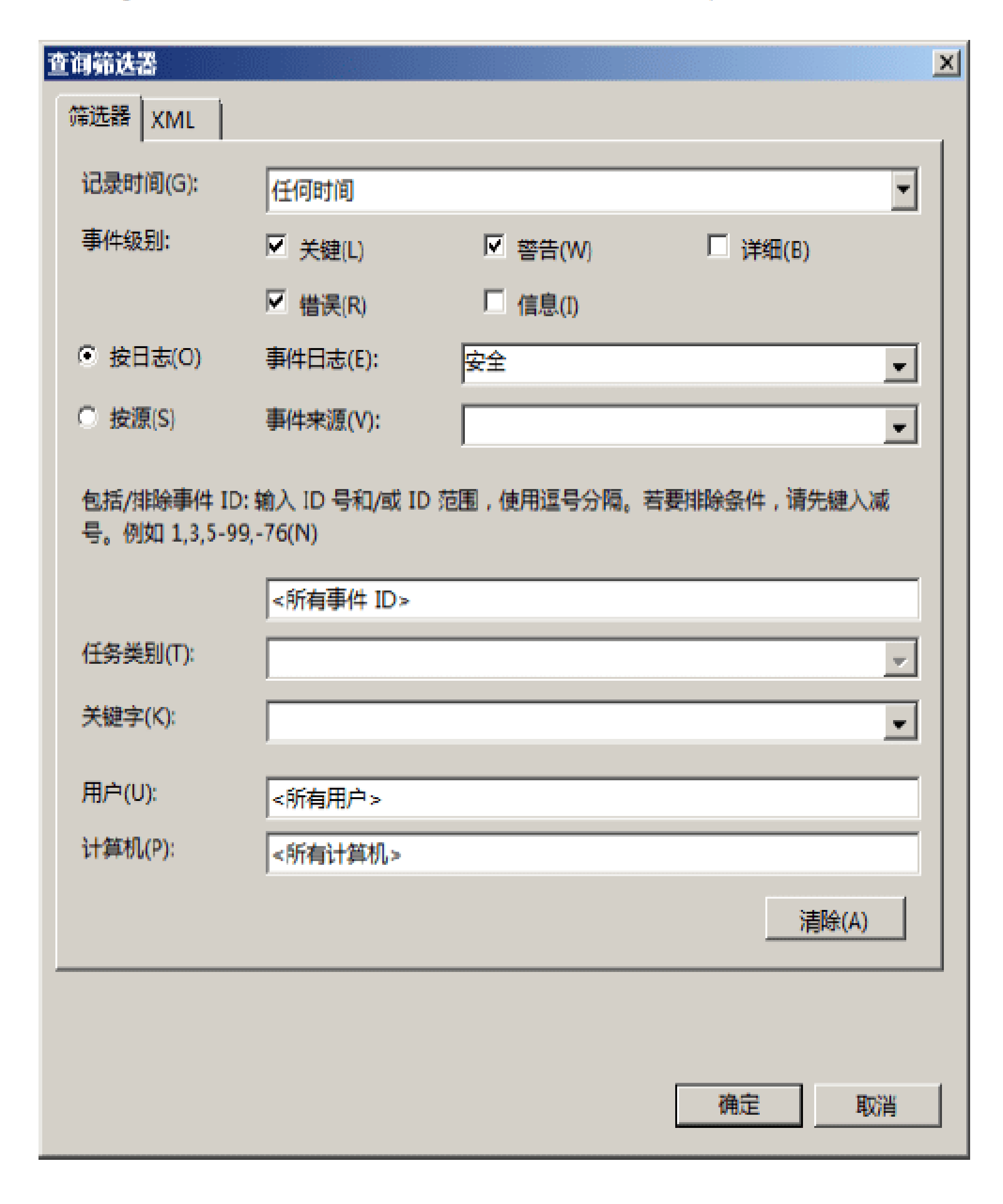


图 18.42 “查询筛选器”对话框

07 单击“确定”按钮，返回“订阅属性”对话框，单击“高级”按钮，打开如图 18.43 所示“高级订阅设置”对话框。由于已经将事件收集服务器的计算机帐户添加到了源计算机的 Administrators 组中，所以选择“计算机帐户”单选按钮即可。

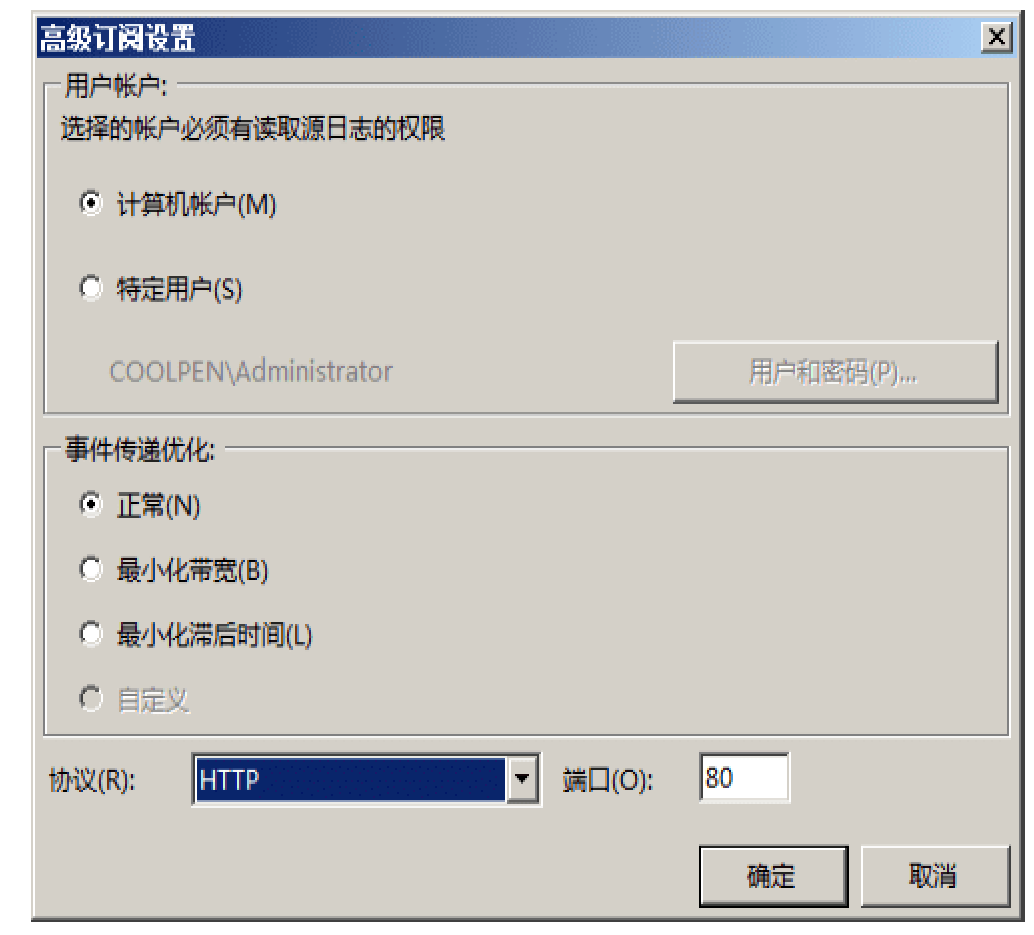


图 18.43 “高级订阅设置”对话框

- 特定用户。若要指定用于管理收集事件的过程的帐户，则可以选择“特定用户”单选按钮，然后单击“用户和密码”按钮，打开如图 18.44 所示“订阅源的凭据”对话框，输入帐户的用户名和密码即可。



图 18.44 “订阅源的凭据”对话框

- 事件传递优化。在这里用户可以根据网络连接状况设置适当的优化措施。例如，如果不希望占用过多网络带宽，选择“最小化带宽”单选按钮即可。系统默认为“正常”状态，即不进行任何优化。
- 协议。系统默认使用 HTTP 协议传出事件，用户也可以在“协议”下拉列表中选择“HTTPS”协议，但是还必须在 Windows 防火墙的“例外”程序中添加“443 端口”。如果使用“正常”(PULL 模式) 传递优化的订阅，则只需在源计算机的防火墙上设置例外；如果使用“最小化带宽”或“最小化滞后时间”(PUSH 模式) 传递优化的订阅，则必须在源计算机和收集器计算机上同时设置例外。

06 连续单击“确定”按钮返回至“订阅属性”对话框，单击“选择事件”按钮，打开如图 18.42 所示“查询筛选器”对话框。在“记录时间”下拉列表中选择希望收集的事件产生的时间和日期。在“事件级别”选项区域选择被收集事件的级别，选择“按日志”单选按钮，并在“事件日志”下拉列表中，选择事件类型。需要注意的是，如果选择的事件类型过多，可能需要收集大量的事件，占用大量空间。

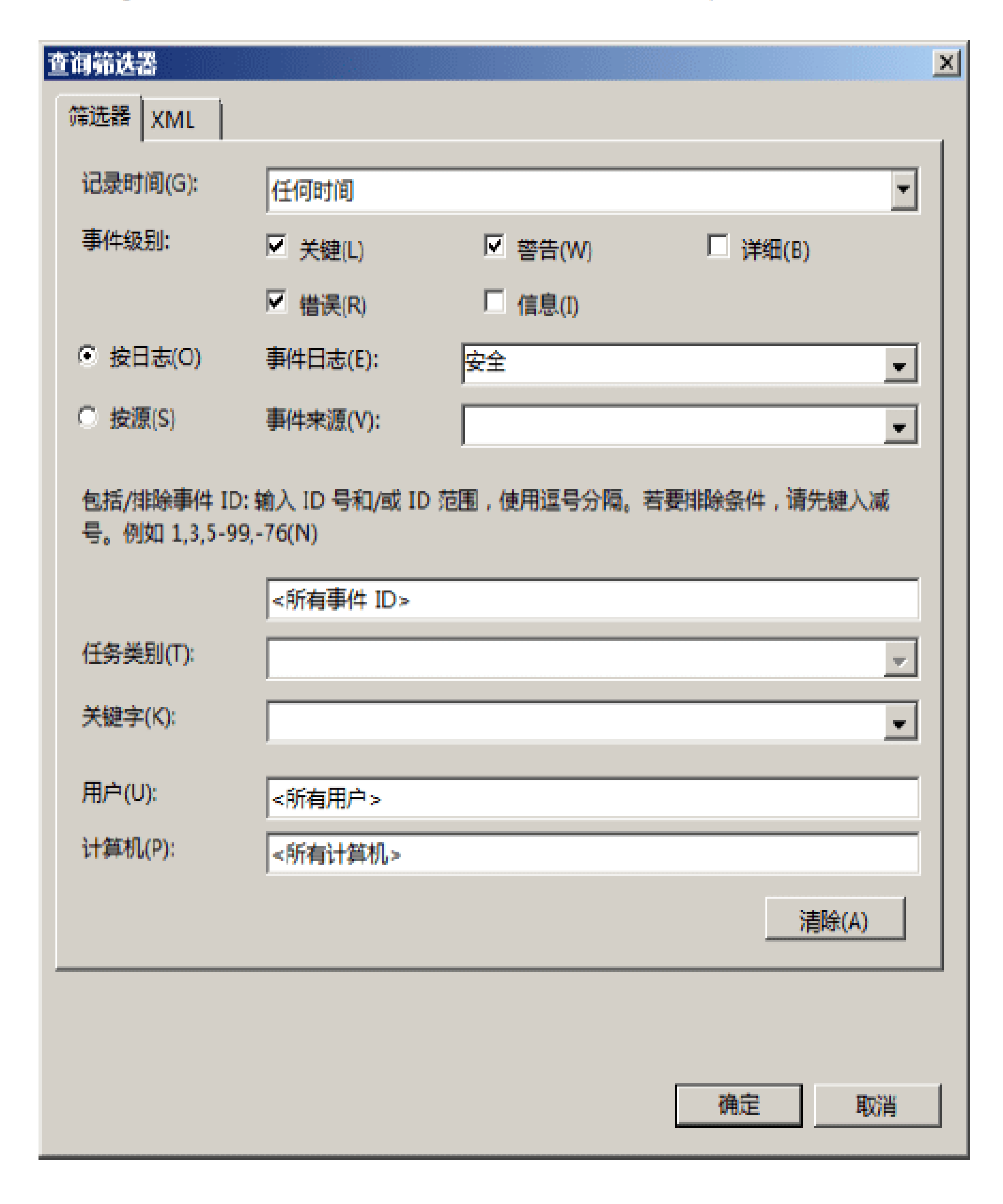


图 18.42 “查询筛选器”对话框

07 单击“确定”按钮，返回“订阅属性”对话框，单击“高级”按钮，打开如图 18.43 所示“高级订阅设置”对话框。由于已经将事件收集服务器的计算机帐户添加到了源计算机的 Administrators 组中，所以选择“计算机帐户”单选按钮即可。

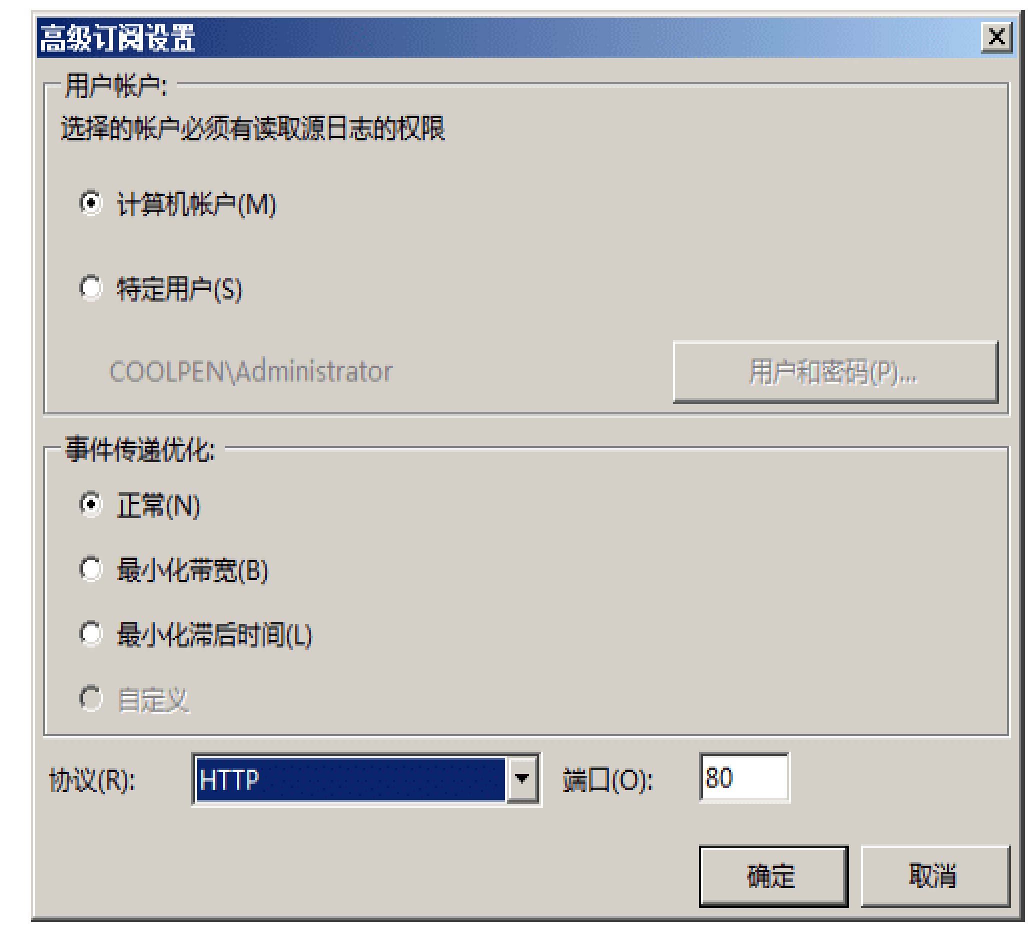


图 18.43 “高级订阅设置”对话框

- 特定用户。若要指定用于管理收集事件的过程的帐户，则可以选择“特定用户”单选按钮，然后单击“用户和密码”按钮，打开如图 18.44 所示“订阅源的凭据”对话框，输入帐户的用户名和密码即可。



图 18.44 “订阅源的凭据”对话框

- 事件传递优化。在这里用户可以根据网络连接状况设置适当的优化措施。例如，如果不希望占用过多网络带宽，选择“最小化带宽”单选按钮即可。系统默认为“正常”状态，即不进行任何优化。
- 协议。系统默认使用 HTTP 协议传出事件，用户也可以在“协议”下拉列表中选择“HTTPS”协议，但是还必须在 Windows 防火墙的“例外”程序中添加“443 端口”。如果使用“正常”（PULL 模式）传递优化的订阅，则只需在源计算机的防火墙上设置例外；如果使用“最小化带宽”或“最小化滞后时间”（PUSH 模式）传递优化的订阅，则必须在源计算机和收集器计算机上同时设置例外。

06 连续单击“确定”按钮返回至“订阅属性”对话框，单击“选择事件”按钮，打开如图 18.42 所示“查询筛选器”对话框。在“记录时间”下拉列表中选择希望收集的事件产生的时间和日期。在“事件级别”选项区域选择被收集事件的级别，选择“按日志”单选按钮，并在“事件日志”下拉列表中，选择事件类型。需要注意的是，如果选择的事件类型过多，可能需要收集大量的事件，占用大量空间。

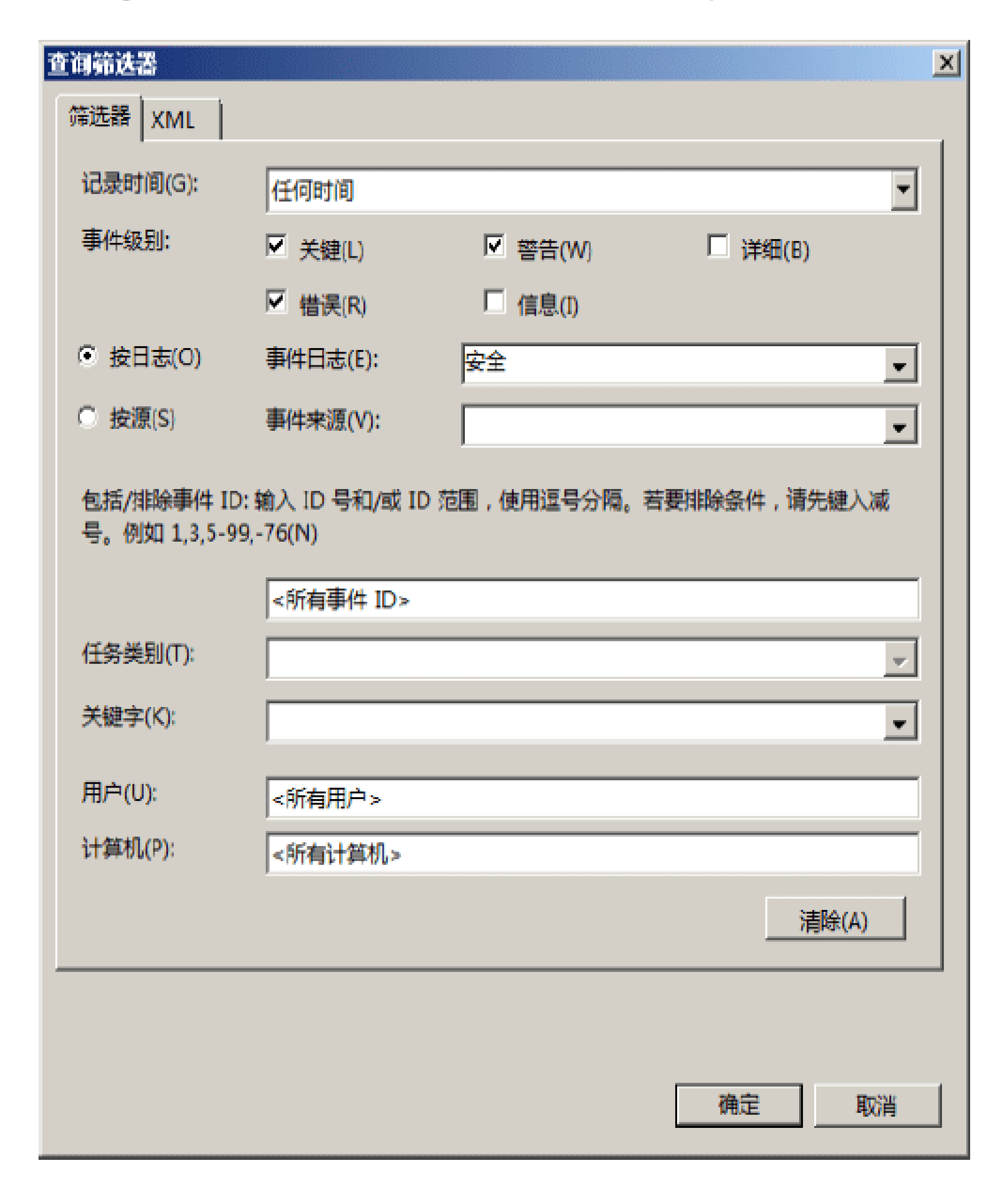


图 18.42 “查询筛选器”对话框

07 单击“确定”按钮，返回“订阅属性”对话框，单击“高级”按钮，打开如图 18.43 所示“高级订阅设置”对话框。由于已经将事件收集服务器的计算机帐户添加到了源计算机的 Administrators 组中，所以选择“计算机帐户”单选按钮即可。

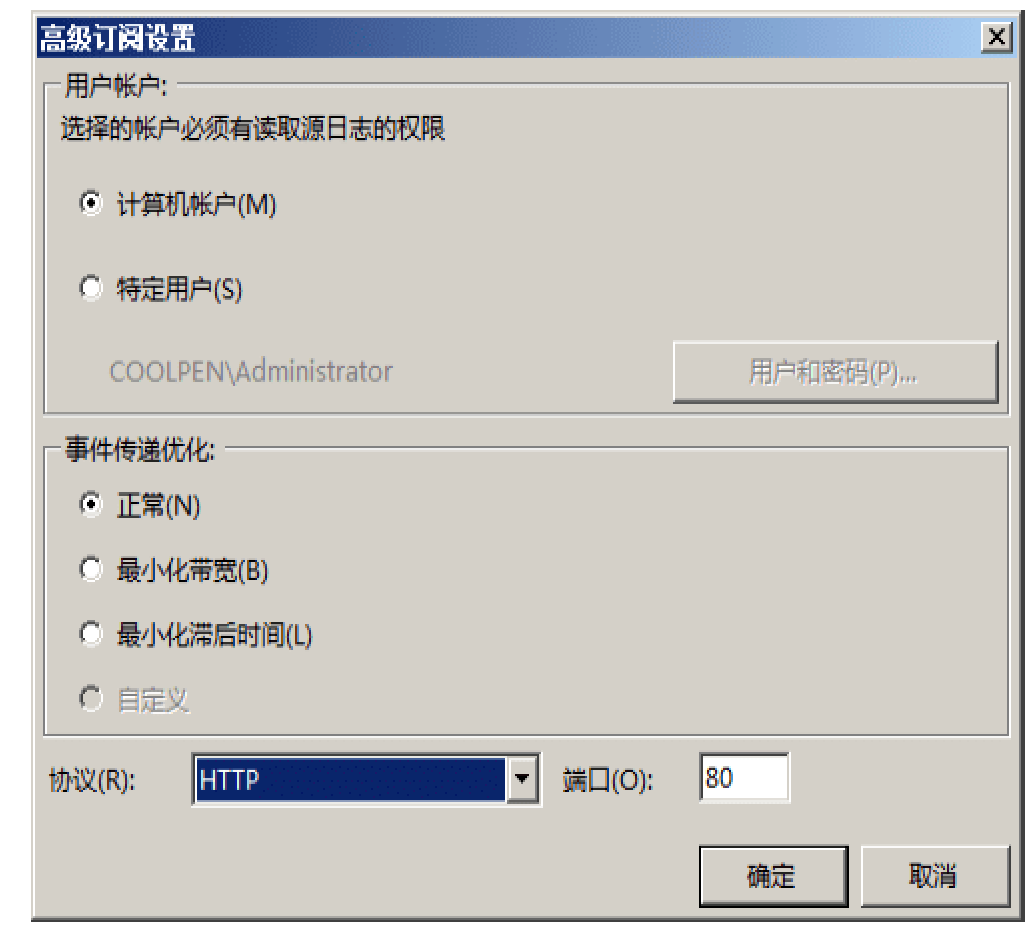


图 18.43 “高级订阅设置”对话框

- 特定用户。若要指定用于管理收集事件的过程的帐户，则可以选择“特定用户”单选按钮，然后单击“用户和密码”按钮，打开如图 18.44 所示“订阅源的凭据”对话框，输入帐户的用户名和密码即可。



图 18.44 “订阅源的凭据”对话框

- 事件传递优化。在这里用户可以根据网络连接状况设置适当的优化措施。例如，如果不希望占用过多网络带宽，选择“最小化带宽”单选按钮即可。系统默认为“正常”状态，即不进行任何优化。
- 协议。系统默认使用 HTTP 协议传出事件，用户也可以在“协议”下拉列表中选择“HTTPS”协议，但是还必须在 Windows 防火墙的“例外”程序中添加“443 端口”。如果使用“正常”（PULL 模式）传递优化的订阅，则只需在源计算机的防火墙上设置例外；如果使用“最小化带宽”或“最小化滞后时间”（PUSH 模式）传递优化的订阅，则必须在源计算机和收集器计算机上同时设置例外。

06 连续单击“确定”按钮返回至“订阅属性”对话框，单击“选择事件”按钮，打开如图 18.42 所示“查询筛选器”对话框。在“记录时间”下拉列表中选择希望收集的事件产生的时间和日期。在“事件级别”选项区域选择被收集事件的级别，选择“按日志”单选按钮，并在“事件日志”下拉列表中，选择事件类型。需要注意的是，如果选择的事件类型过多，可能需要收集大量的事件，占用大量空间。

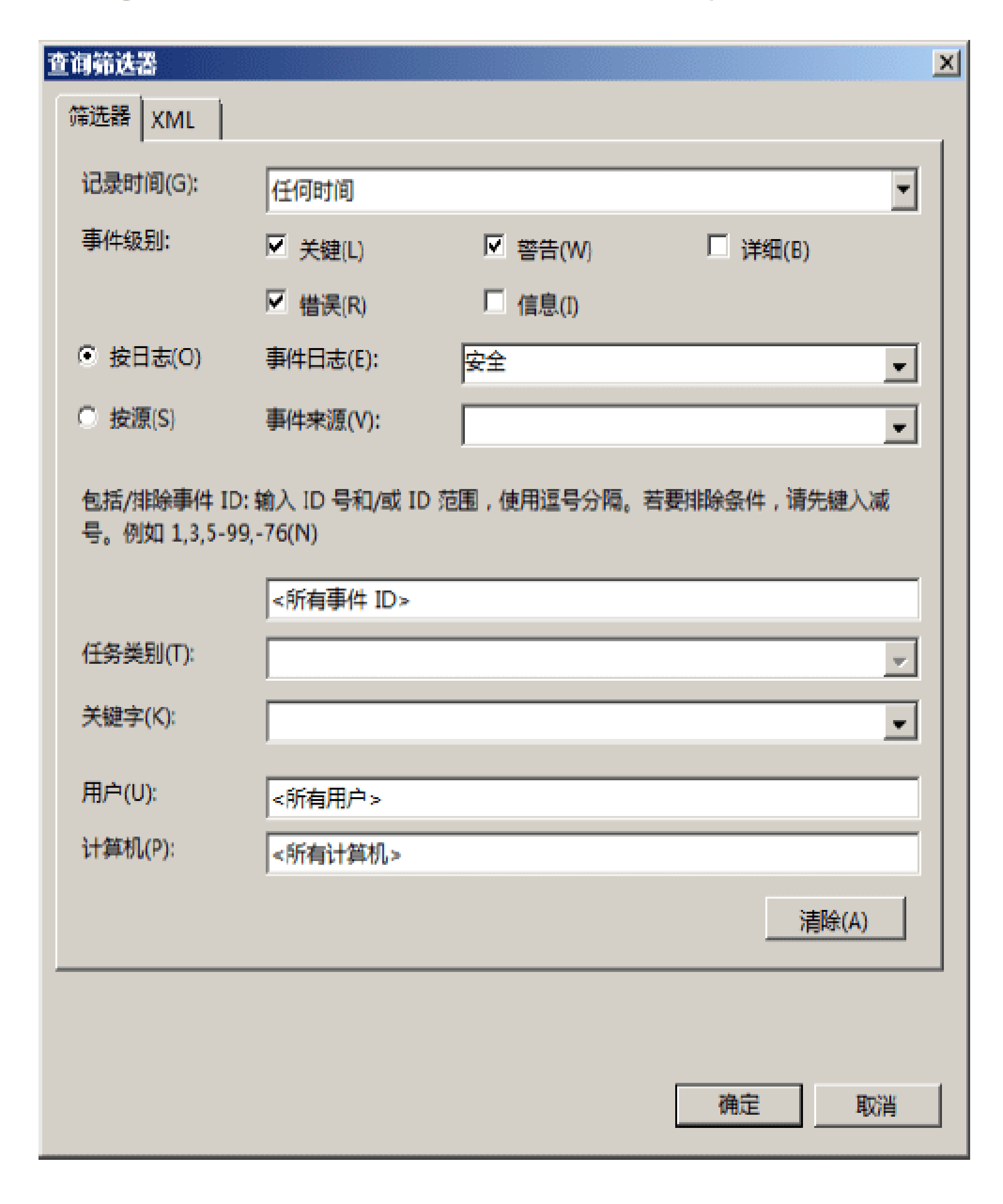


图 18.42 “查询筛选器”对话框

07 单击“确定”按钮，返回“订阅属性”对话框，单击“高级”按钮，打开如图 18.43 所示“高级订阅设置”对话框。由于已经将事件收集服务器的计算机帐户添加到了源计算机的 Administrators 组中，所以选择“计算机帐户”单选按钮即可。

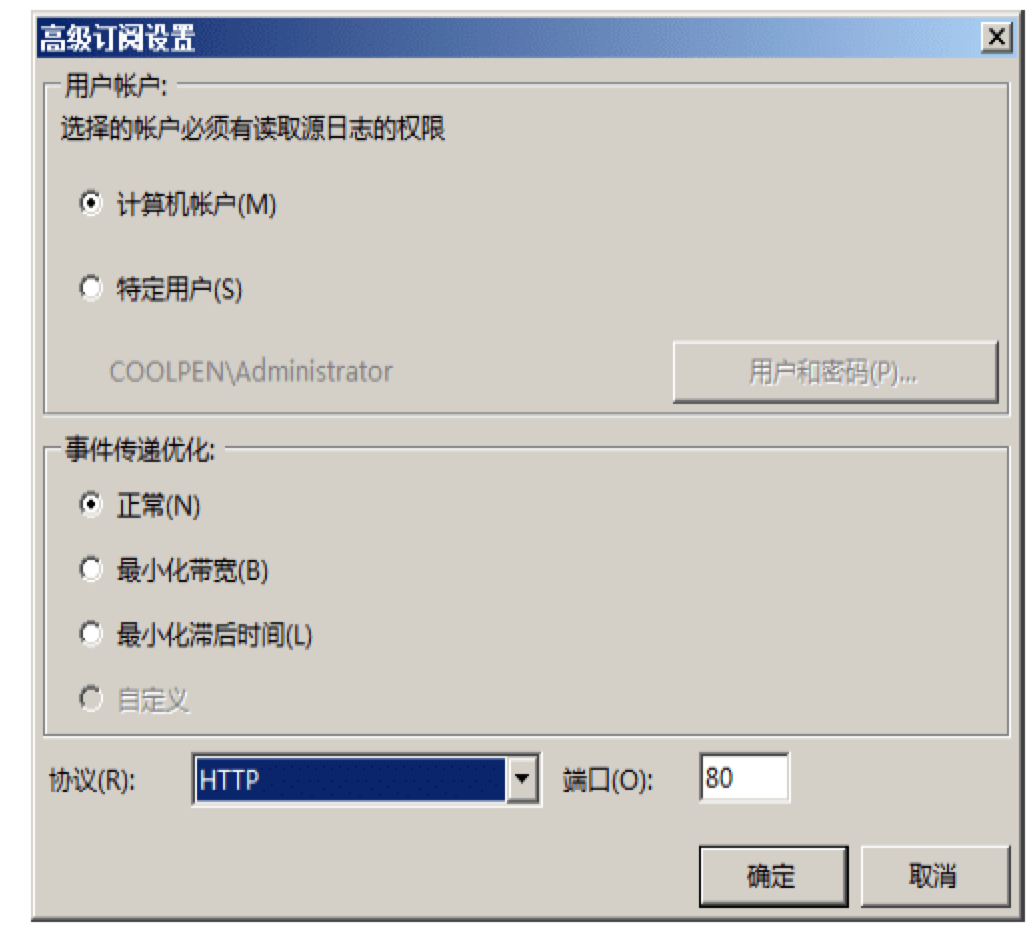


图 18.43 “高级订阅设置”对话框

- 特定用户。若要指定用于管理收集事件的过程的帐户，则可以选择“特定用户”单选按钮，然后单击“用户和密码”按钮，打开如图 18.44 所示“订阅源的凭据”对话框，输入帐户的用户名和密码即可。



图 18.44 “订阅源的凭据”对话框

- 事件传递优化。在这里用户可以根据网络连接状况设置适当的优化措施。例如，如果不希望占用过多网络带宽，选择“最小化带宽”单选按钮即可。系统默认为“正常”状态，即不进行任何优化。
- 协议。系统默认使用 HTTP 协议传出事件，用户也可以在“协议”下拉列表中选择“HTTPS”协议，但是还必须在 Windows 防火墙的“例外”程序中添加“443 端口”。如果使用“正常”（PULL 模式）传递优化的订阅，则只需在源计算机的防火墙上设置例外；如果使用“最小化带宽”或“最小化滞后时间”（PUSH 模式）传递优化的订阅，则必须在源计算机和收集器计算机上同时设置例外。

06 连续单击“确定”按钮返回至“订阅属性”对话框，单击“选择事件”按钮，打开如图 18.42 所示“查询筛选器”对话框。在“记录时间”下拉列表中选择希望收集的事件产生的时间和日期。在“事件级别”选项区域选择被收集事件的级别，选择“按日志”单选按钮，并在“事件日志”下拉列表中，选择事件类型。需要注意的是，如果选择的事件类型过多，可能需要收集大量的事件，占用大量空间。

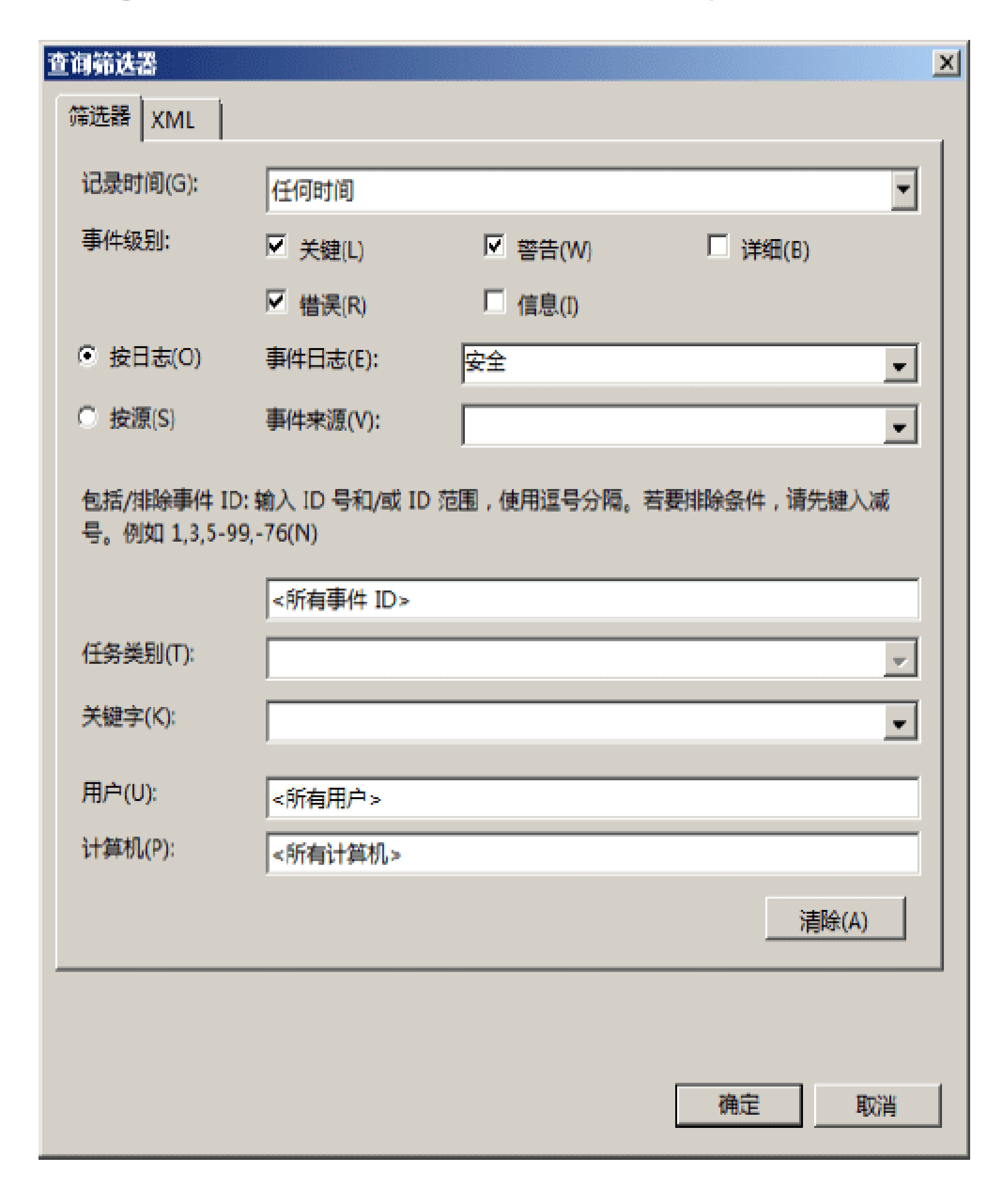


图 18.42 “查询筛选器”对话框

07 单击“确定”按钮，返回“订阅属性”对话框，单击“高级”按钮，打开如图 18.43 所示“高级订阅设置”对话框。由于已经将事件收集服务器的计算机帐户添加到了源计算机的 Administrators 组中，所以选择“计算机帐户”单选按钮即可。

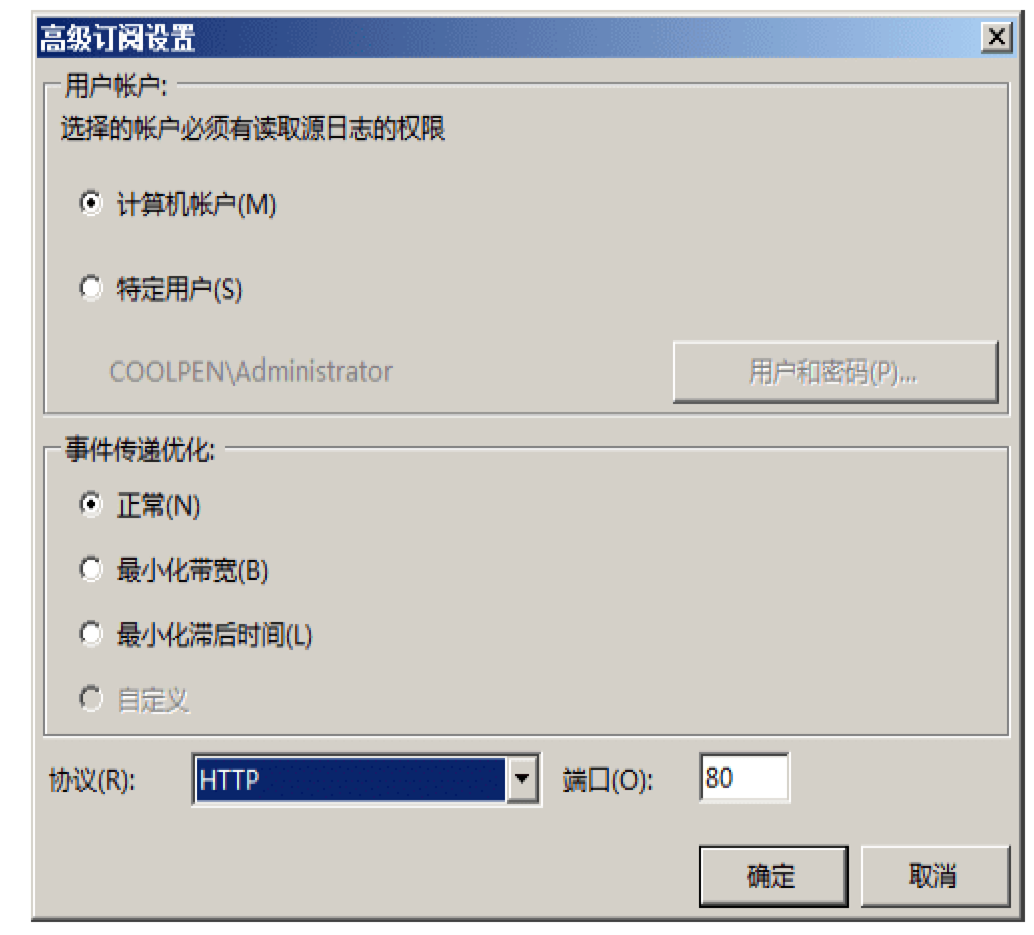


图 18.43 “高级订阅设置”对话框

- 特定用户。若要指定用于管理收集事件的过程的帐户，则可以选择“特定用户”单选按钮，然后单击“用户和密码”按钮，打开如图 18.44 所示“订阅源的凭据”对话框，输入帐户的用户名和密码即可。
- 事件传递优化。在这里用户可以根据网络连接状况设置适当的优化措施。例如，如果不希望占用过多网络带宽，选择“最小化带宽”单选按钮即可。系统默认为“正常”状态，即不进行任何优化。



图 18.44 “订阅源的凭据”对话框

- 协议。系统默认使用 HTTP 协议传出事件，用户也可以在“协议”下拉列表中选择“HTTPS”协议，但是还必须在 Windows 防火墙的“例外”程序中添加“443 端口”。如果使用“正常”（PULL 模式）传递优化的订阅，则只需在源计算机的防火墙上设置例外；如果使用“最小化带宽”或“最小化滞后时间”（PUSH 模式）传递优化的订阅，则必须在源计算机和收集器计算机上同时设置例外。



08 单击“确定”按钮，关闭“订阅属性”对话框，返回“事件查看器”窗口，如图 18.45 所示，新创建的事件订阅已经显示在窗口中。

09 通过事件查看器订阅的远程计算机日志，默认将显示在“Windows 日志”的“转发的事件”项目中，如图 18.46 所示。需要注意的是，由于网络传输等多方面问题，远程计算机上产生的相关事件并不能立即转发到事件收集服务器上，通常会有一定时间的延迟。

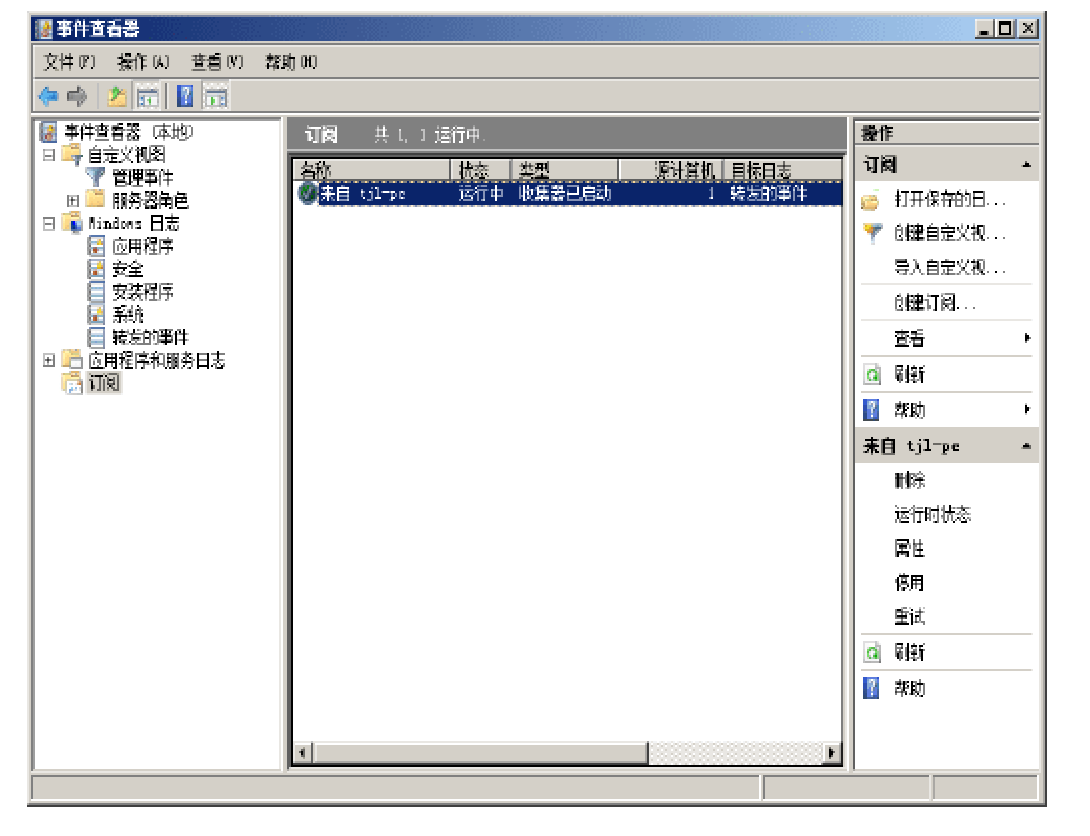




图 18.45　成功创建的订阅

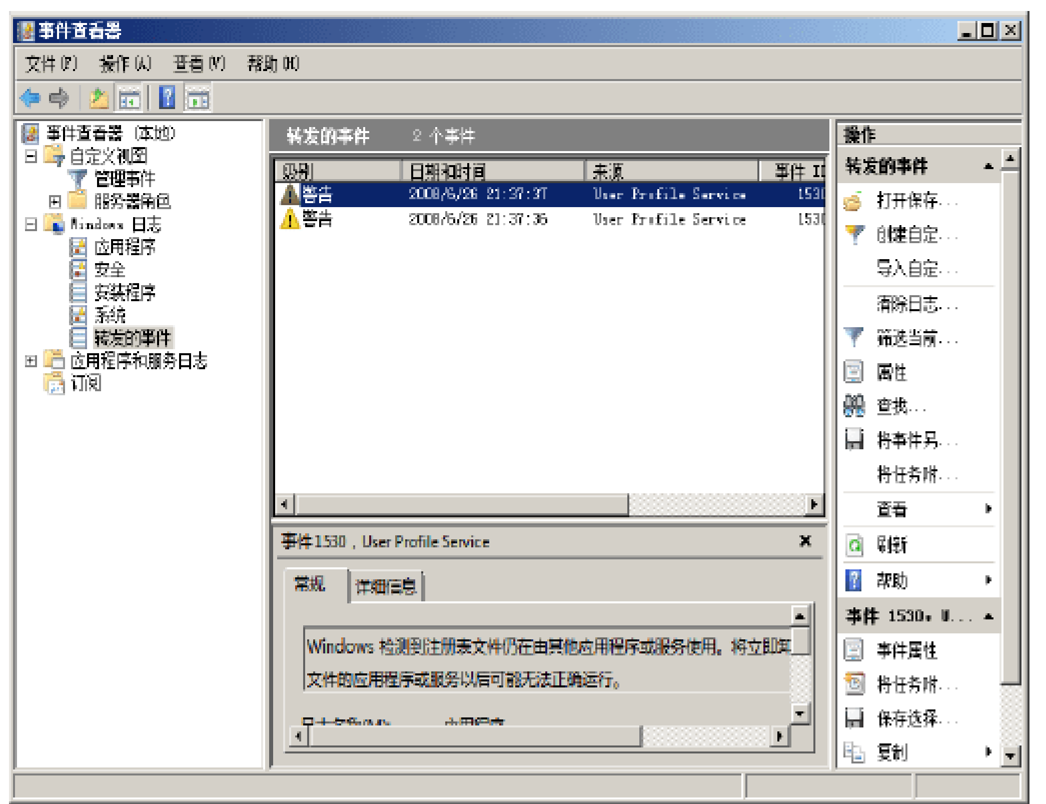


图 18.46　转发的事件

18.2.5　可靠性和性能监视器

可靠性和性能监视器可以帮助管理员轻松监控与分析系统性能。Windows Server 2008 的可靠性与性能监视器是 MMC 的一个插件，将性能日志与警报、服务器性能顾问以及系统监控器结合在一起，为定制数据收集及时间跟踪服务提供了一个易于使用的图形界面，如图 18.47 所示。它还包含一个可靠性监视器，这是另一个跟踪系统修改并将这些修改与系统可靠性的修改进行对比的 MMC 插件。

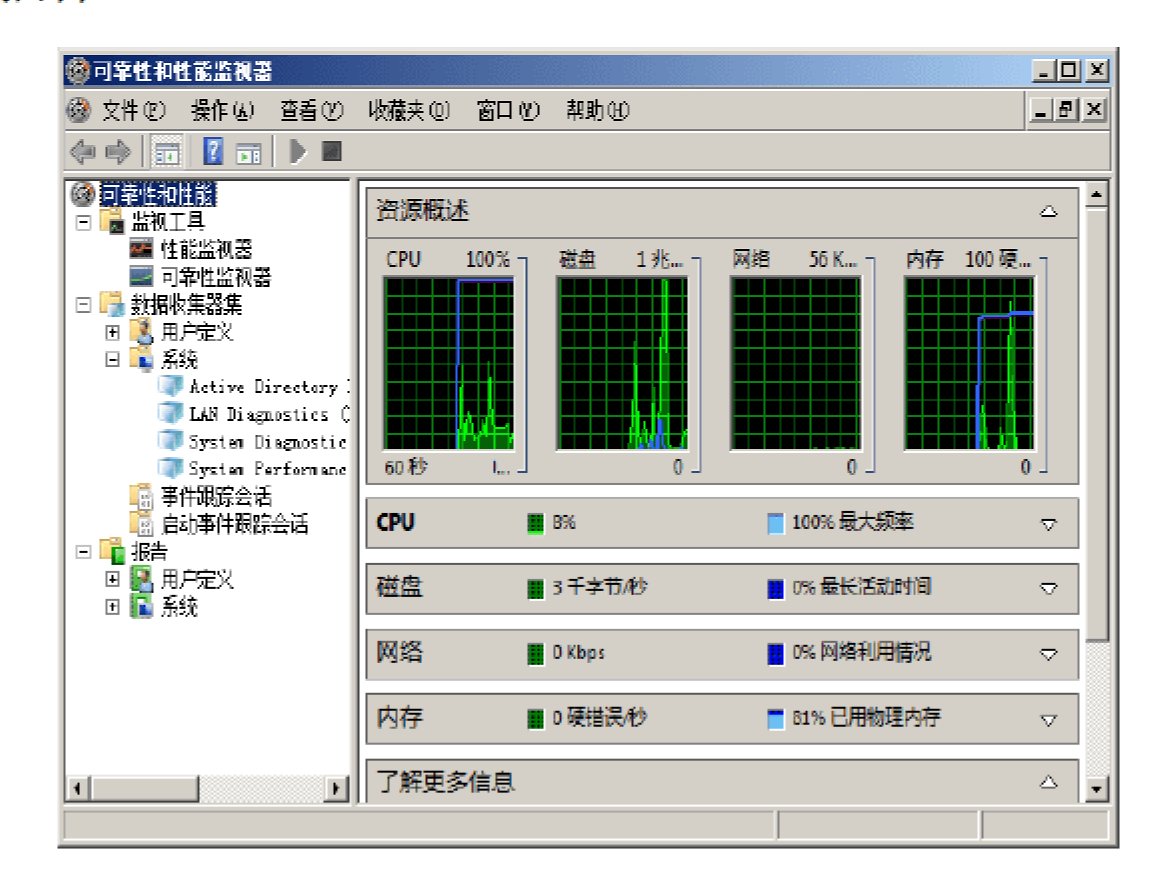


图 18.47　“可靠性和性能监视器”窗口

Windows Server 2008 中的可靠性与性能监视器有如下新特性。

1. 数据收集器

数据收集器是 Windows 可靠性和性能监视器中一个重要的新特征，它将数据收集分成组，形成适用于不同性能与监控条件下的可重复使用的构件。对于管理多个服务器的管理员来说，这种功能明确了需要监控的数据，以及使用在多个服务器上的数据，从而为管理员节省大量时间。当一组数据作为数据收集器被储存时，像调整时间这样的操作就能够通过一个属性更改而应用于整个组，Windows 可靠性和性能监视器还包含一个默认的数据收集器模板，管理员使用它能够立刻开始为某个服务器角色或监控情景进行性能数据的收集。

2. 创建日志的向导与模板

现在，通过一个简化了的向导界面就可以添加计数器到日志文件，并规定开始、停止以及持续的时间。将这个配置保存为模板可以使系统管理员在后面的计算机上搜集同样的日志，而不必在每个计算机上都进行配置。性能日志与提醒功能也被集成到 Windows 可靠性和性能监视器中，与数据收集器共同使用。

3. 资源查看

新的资源查看界面现在成为了 Windows 可靠性和性能监视器的主页。这个界面提供了实时的对 CPU、磁盘、网络和内存占用情况的查看。通过将这些受到监控的内容进行扩展，可使系统管理员确认哪些流程在使用哪些资源。在 Windows 之前的版本中，这一实时的根据流程确定的数据只在有限的任务管理器的表格中存在。

4. 可靠性监视器

可靠性监视器通过计算系统的可靠性参数来反映是否有不可预见的问题降低了系统的可靠性。按时间计算的可靠性参数图表明了问题开始出现的日期。系统稳定性报告提供了详细的信息，用以帮助从根源上解决问题。通过查看对系统的更改，能够很快找到解决问题的策略，节省时间与资源。

5. 为数据搜集进行属性配置

无论是一次性使用创建数据收集器，还是持续地将行为记录到日志，用于创建、修改和安排日程的界面都是相同的。如果数据收集器被证明对未来的性能监控有用，那么它就无需再次创建，可直接把它作为模板重新配置或保存。这种简化的流程将节省管理员的时间，提供更有效的性能监控信息。

6. 诊断报告

熟悉 Windows Server 2003 中的服务器性能顾问的用户会在 Windows Server 2008 的 Windows 可靠性和性能监视器中找到相同类型的诊断报告。生成报告所需的时间也得到了改进。报告可以根据通过使用任何数据收集器收集的数据来创建，使系统管理员能够轻松地复制



报告，并评估对服务器的修改是如何影响性能的，以及查看报告推荐的解决方案。

18.3　应用服务器角色安全新特性

Windows Server 2008 强大的网络服务功能也是吸引众多用户的主要方面，在对原有网络服务进行升级和改进的基础上，还重新集成了更多的网络应用，充分满足各种规模网络用户的需求。

18.3.1　活动目录域服务

通过实践不难发现，Windows Server 2008 系统中的 Active Direcotory 服务变化的不仅是名称，更重要的是功能，尤其是安全性和可靠性的提升。在活动目录方面，Windows Server 2008 引入了全新的只读域控制器技术、可重启的 AD DS 技术、目录服务审计等一系列新功能。

1. AD FS

Active Directory Federation Services（AD FS）是 Windows Server 2008 中的一种服务器角色，可提供一种有较高可扩展性的安全身份访问解决方案，支持在不同平台上工作。AD FS 使网络内外基于浏览器的客户端能访问受保护的因特网应用，即便用户帐户和应用位于不同网络和企业中也能保证其正常工作。

在一般情况下，应用位于某个网络，而用户帐户位于另一个网络，这时用户要想访问应用的话，就必须输入辅助凭据。但是，如果我们采用了 AD FS，就不再需要辅助凭据了。我们可利用受信任的关系来向受信任合作伙伴呈现用户数字身份和访问权限。在联合环境中，每个企业不仅能够一如既往地管理其自己的身份，而且还能安全地规划和接受其他企业的身份。

AD FS 包括一种策略导入/导出特性，简化不同联合合作伙伴间设置信任关系的工作。对于来自联合合作伙伴的用户，成员供应商可支持对 Windows SharePoint Services（WSS）与 RMS 基于角色的授权。管理员能通过组策略控制联合服务部署。

此外，拥有和管理用户帐户的企业可采用 AD FS 联合服务器来验证本地用户并创建安全令牌。企业资源的联合服务器可用上述安全令牌来作出授权决策。

2. 可以重启的 AD DS

在 Windows Server 2008 中，Active Directory Domain Services（AD DS）是基于服务的，也就是说，我们可通过 Microsoft Management Console（MMC）管理单元/命令行关闭或启动它。基于服务的 AD DS 简化了管理工作，缩短了执行脱机工作所需的时间，如脱机碎片整理或权限恢复等。此外，这也有助于提高运行于域控制器上的其他服务的可用性，条件是在执行 AD DS 维护的同时，应保持这些服务始终处于活动状态。任何绑定于已经停机的域控制器上的客户端都能通过发现转移到其他域控制器上工作。

3. RODC

只读域控制器（RODC）是 Windows Server 2008 操作系统中的一种新型域控制器，用于部署在需要本地验证服务而物理安全级又难以保证的分支机构中。除了帐户密码之外，RODC 还包括可写入域控制器中的全部 Microsoft Active Directory Domain Services（AD DS）对象和属性。但是，客户端不能直接写入修改 RODC。这就提高了安全性，因为即便物理安全被破坏，有人恶意存取 RODC，域数据也不会在 RODC 上更新。

RODC 还支持管理员角色分隔，这样，包括分支机构本地用户在内的任何域用户都可获得授权成为 RODC 的本地管理员，同时又不会给予用户更多域本身或其他域控制器的管理权限。本地员工只能执行更新驱动程序等例行管理任务，而不会影响安全性。

18.3.2 AD DS 审核

在 Windows Server 2008 中，管理员审核活动目录对象有多种选择。新的审核策略子目录可审核活动目录对象的变化，包括创建、修改、移动和删除等，并能将发生变化的新旧属性值计入日志。需要注意的是，这种审核功能仅适用于目录服务对象访问，并不适用于文件系统对象以及注册表对象。

1. 审核 AD DS 访问

在 Windows 2000 Server 和 Windows Server 2003 中，只有一个审核策略，即审核目录服务访问，它控制着目录服务审核事件是否启用。在 Windows Server 2008 中，这个策略则分为 4 个子目录：

- 目录服务访问（Directory Service Access）；
- 目录服务变化（Directory Service Changes）；
- 目录服务复制（Directory Service Replication）；
- 详细的目录服务复制（Detailed Directory Service Replication）。

全局审核策略 Audit Directory Service Access 控制着目录服务审核是否启用。这一安全设置决定了目录中对象执行特定操作时事件是否记入安全日志。管理员可通过修改对象的系统访问控制列表（SACL）来控制审核哪些操作。AD DS 对象上的 SACL 可在对象属性对话框中的安全选项卡中设置。在 Windows Server 2008 中，该策略默认是启用的。

如果通过修改默认的域控制器对策略制定该策略设置，则管理员可以指定审核是成功还是失败，或者不进行审核。用户成功访问指定了 SACL 的 AD DS 对象后，成功审核会生成相应审核项。如果用户失败访问指定了 SACL 的 AD DS 对象后，则审核失败也会生成相应审核项。在 Windows 2000 Server 和 Windows Server 2003 中，审核事件出现在安全日志中，ID 号为 566。在 Windows Server 2008 中，审核子目录“目录服务访问”仍生成同样的事件，但事件 ID 号改为 4662。

2. 审核 AD DS 变动

新的审核子目录 Directory Service Change 支持审核 AD DS 中对象的变动情况。可审核的变动类型包括对象的创建、修改、移动和反删除操作等。这些操作生成的事件出现在安全日



志中，并包括先前的和当前的属性值。

这种新策略子目录为 AD DS 审核添加了以下功能：

- 成功修改对象的属性值后，AD DS 会将先前的和当前的属性值记入日志。如果属性值多于一个，那么只有修改操作造成变化的值才记入日志；
- 如果创建新的对象，那么创建时会给对象属性赋值，并记入日志。如果在创建过程中添加属性，那么这些新的属性值会记入日志。在大多数情况下，AD DS 会给属性分配默认值（如 sAMAccountName）。这种系统属性值不记入日志；
- 如果对象在域中移动，那么此前的位置和新的位置会（以区别名的形式）记入日志。如果对象移动到不同的域，那么会在目标域的域控制器上生成创建事件；
- 如果对对象进行反删除操作，那么对象移动的位置会记入日志。此外，如果在反删除操作中添加、修改或删除属性，那么这些属性值也会记入日志。

如果对象被删除，不会生成改变审核事件。但是，如果启用了目录服务访问子目录，会生成审核事件。启用“目录服务更改”审核策略后，如果管理员设置进行审核的对象发生变动，那么 AD DS 会将事件记入安全事件日志中。

3. 全局审核策略

启用全局审核策略后，可支持所有目录服务策略子目录。全局审核策略可在默认域控制器组策略中设置（在“安全配置”→“本地策略”→“审核策略”分支下）。

在 Windows Server 2008 中，全局审核策略是默认启用的。因此，目录服务变化（Directory Service Changes）子目录也是默认启用的。这个子目录仅对审核成功事件设置。管理员可选择禁用的目录服务访问（Directory Service Access）。

在 Windows 2000 Server 和 Windows Server 2003 中，“审核目录服务访问”审核策略是活动目录可用的唯一审核控件。该控件生成的事件不会显示任何修改的新旧值。利用新的审核策略子目录服务变化，将成功的目录修改记入到日志的同时，也会记入以前的与当前的属性值。由于现在我们可以记录对象属性的变化，因此改善了事件日志的用途，可用它作为跟踪对象使用过程中变化情况的一种机制，并能根据需要将对象属性变为以前的值。

18.3.3　Active Directory 权限管理服务

Active Directory 权限管理服务（Active Directory Rights Management Services，AD RMS）是 Windows Server 2008 的新增功能之一。这是一种信息保护技术，与启用 RMS 的应用程序配合使用，可帮助保护数字信息避免未经授权的使用。

1. AD RMS 的新特性

AD RMS 与 RMS 相比具有如下新特性：

- 管理界面更加友好。在 RMS 1.0 中唯一的管理界面就是 Web，而 AD RMS 则改用 MMC



志中，并包括先前的和当前的属性值。

这种新策略子目录为 AD DS 审核添加了以下功能：

- 成功修改对象的属性值后，AD DS 会将先前的和当前的属性值记入日志。如果属性值多于一个，那么只有修改操作造成变化的值才记入日志；
- 如果创建新的对象，那么创建时会给对象属性赋值，并记入日志。如果在创建过程中添加属性，那么这些新的属性值会记入日志。在大多数情况下，AD DS 会给属性分配默认值（如 sAMAccountName）。这种系统属性值不记入日志；
- 如果对象在域中移动，那么此前的位置和新的位置会（以区别名的形式）记入日志。如果对象移动到不同的域，那么会在目标域的域控制器上生成创建事件；
- 如果对对象进行反删除操作，那么对象移动的位置会记入日志。此外，如果在反删除操作中添加、修改或删除属性，那么这些属性值也会记入日志。

如果对象被删除，不会生成改变审核事件。但是，如果启用了目录服务访问子目录，会生成审核事件。启用“目录服务更改”审核策略后，如果管理员设置进行审核的对象发生变动，那么 AD DS 会将事件记入安全事件日志中。

3. 全局审核策略

启用全局审核策略后，可支持所有目录服务策略子目录。全局审核策略可在默认域控制器组策略中设置（在“安全配置”→“本地策略”→“审核策略”分支下）。

在 Windows Server 2008 中，全局审核策略是默认启用的。因此，目录服务变化（Directory Service Changes）子目录也是默认启用的。这个子目录仅对审核成功事件设置。管理员可选择禁用的目录服务访问（Directory Service Access）。

在 Windows 2000 Server 和 Windows Server 2003 中，“审核目录服务访问”审核策略是活动目录可用的唯一审核控件。该控件生成的事件不会显示任何修改的新旧值。利用新的审核策略子目录服务变化，将成功的目录修改记入到日志的同时，也会记入以前的与当前的属性值。由于现在我们可以记录对象属性的变化，因此改善了事件日志的用途，可用它作为跟踪对象使用过程中变化情况的一种机制，并能根据需要将对象属性变为以前的值。

18.3.3　Active Directory 权限管理服务

Active Directory 权限管理服务（Active Directory Rights Management Services，AD RMS）是 Windows Server 2008 的新增功能之一。这是一种信息保护技术，与启用 RMS 的应用程序配合使用，可帮助保护数字信息避免未经授权的使用。

1. AD RMS 的新特性

AD RMS 与 RMS 相比具有如下新特性：

- 管理界面更加友好。在 RMS 1.0 中唯一的管理界面就是 Web，而 AD RMS 则改用 MMC

嵌入式管理单元，操作更加方便；

- 自动启用服务器授权凭证。在 AD RMS 中，根群集的服务器授权凭证（Server Licensor Certificate，SLC）可以自动启用，无需再进行手动操作；
- 与 Active Directory 联合身份验证服务(AD FS)配合使用。AD FS 是 Windows Server 2008 的一项新功能，可以提供简单、安全的身份验证。AD RMS 与 AD FS 配合使用，可以允许企业之间共同使用一方的 AD RMS 群集，并且通过 AD FS（使用 https 协议）对自己域中的用户帐户进行识别和验证。

2. AD RMS 的相关组件

AD RMS 仍然基于服务器/客户机的结构，其主要组件包括支持 AD RMS 的应用程序、AD RMS 客户端和 AD RMS 服务器端 3 项，三者缺一不可。只有支持 AD RMS 的应用程序才能生成被保护的文档；AD RMS 客户端安装在客户机上，与支持 AD RMS 的应用程序进行交互；AD RMS 服务器负责为信任实体颁发证书、授权服务器，为 AD RMS 保护的文档进行使用授权。

使用权限管理帐户证书可以将用户帐户和具体的一台设备关联起来，也就是说每个不同的帐户在同一台计算机上存在唯一的权限管理证书，或同一帐户在不同的计算机上的权限管理证书也不相同。虽然不同用户的权限管理帐户证书不同，但是在权限管理帐户证书中所包含的密钥却是相同的。该权限管理帐户证书是由企业中的第一台 AD RMS 服务器所颁发的，即在任何计算机上的用户的密钥都是相同的，当用户向 AD RMS 许可服务器请求许可时，就需要使用权限管理帐户证书。

RAC 的生成过程如下：

01 当用户第一次使用由 AD RMS 加密的文档时，就需要向 AD RMS 服务器发送请求，首先用户会以域用户的身份向 AD RMS 证书服务器发送请求，来获取权限管理帐户证书。

02 服务器会在服务器数据库中对所存的信息进行查询，如果已经存在密钥对，就会应用已有的密钥，如果没有就会为该用户生成一个密钥对。

03 服务器会将该用户的密钥对中的私钥用该证书服务器的私钥进行加密。

04 将用户密钥对中的私钥加密后，服务器会将用户密钥对中的公钥和加密后的私钥放到权限管理帐户证书中。

05 权限管理帐户证书会被 AD RMS 服务器用私钥进行数字签署，这样就能确定该权限管理帐户证书是由 AD RMS 证书服务器所发放的，且没有被篡改。

06 AD RMS 服务器会将权限管理帐户证书发送给用户。

07 服务器将用户的密钥对存储到 AD RMS 的数据库中，该权限管理帐户证书就是以后该用户申请各种使用许可的证书。

3. AD RMS 的实现原理

（1）服务的发现

服务的发现实际上就是 RMS 客户端发现 AD RMS 服务器的一个过程，该过程可以通过两种方法来实现，一种是通过活动目录中的服务连接点（SCP），通过它就可以找到我们企业中的证书服务器的位置。第二种方法就是通过注册表，通过注册表可以使客户端上的应用程序找



到 AD RMS 服务器。

找到 AD RMS 服务器可以激活 RMS 客户机，因为如果要使用该 RMS 客户机必须在第一次使用时到 AD RMS 服务器上去激活该 RMS 客户机。这样就可以从 AD RMS 服务器上获取权限管理帐户证书等信息。

（2）文档的在线发布过程

由 RMS 客户端在线向授权服务器发送请求。具体的发布过程如下：

01 由密码箱生成对称密钥作为内容密钥。
02 内容密钥会被授权服务器的公钥加密，这样做的目的就是通过网络将它发送给授权服务器，然后授权服务器能够用它自己的私钥将这个内容解出来，而在传送的过程中不会被别人截获后获取内容密钥。
03 加密的内容密钥和权限被发送给请求发布许可的授权服务器。
04 授权服务器使用它的私钥解开加密的内容密钥。
05 授权服务器使用它的公钥加密内容密钥和使用权限。
06 加密后的密钥和使用权限被添加到发布许可。
07 授权服务器使用私钥签署发布许可。
08 发布许可返回给申请的客户端。
09 支持 AD RMS 的应用程序将发布许可合并到受保护的文档中。

（3）文档的离线发布过程

如果用户所使用的是笔记本等移动办公设备，有可能在自己的家中不能够连接到公司的 AD RMS 服务器，这时用户只要申请一个客户端许可证书（CLC），就可以访问公司的 AD RMS 服务器。具体的发布过程如下：

01 由密码箱生成对称密钥作为内容密钥。
02 从客户端许可证书中取出授权服务器的公钥。
03 客户端使用服务器的公钥加密内容密钥，用服务器的公钥加密的内容密钥只能由服务器的私钥解密。
04 客户端使用客户端许可证书的公钥对内容密钥再进行一次加密，会再次获得一个加密后的对称密钥。需要注意的是，离线发布和在线发布所不同的是，在离线发布过程中，对内容进行了两次加密。
05 两个加密后的对称密钥同时被放到发布许可中。
06 客户端使用权限管理帐户证书中的私钥解密客户端许可证书中的私钥。
07 客户端使用 CLC 的私钥签署发布许可。
08 支持 AD RMS 的应用程序将发布许可合并到受保护的文档中。

（4）受保护文档的使用过程

使用受保护文档的过程如下：

01 客户端将权限管理帐户证书和文档的发布许可发送到颁发发布许可的授权服务器。
02 授权服务器使用它的私钥解出发布许可中的内容密钥。
03 授权服务器使用权限管理帐户证书中用户的公钥加密内容密钥。

04 把加密的内容密钥和用户的使用权限添加到使用许可。

05 授权服务器使用它的私钥签署使用许可。

06 服务器将该使用许可发送给客户端。

07 密码箱使用计算机的私钥解密保存在权限管理帐户证书中的用户私钥。

08 密码箱使用用户的私钥解密内容密钥。

09 密码箱使用内容密钥解密被加密的受保护内容。

注意



使用服务器的公钥所加密的内容只能由服务器的私钥来解开。

4. AD RMS 部署安全

AD RMS 通常用于保护企业内部重要数据的信息安全，要求采取与结构中其他关键服务器相同的物理和网络安全措施。在部署 AD RMS 服务过程中，通常可以使用访问控制列表和 SSL 数字加密技术等确保服务器安全。

（1）使用 ACL 限制对 AD RMS 服务站点的访问

管理员可以通过使用访问控制列表限制客户端对 AD RMS 服务站点的访问。在网站上设置 RMS 时创建的每个虚拟目录都具有可保护的相应文件夹结构。该文件夹结构在默认情况下位于<system drive>:\<web_root_folder>_wmcs 中，其中 web_root_folder 是对设置了 RMS 的网站指派的文件夹名称。某些 Web 服务受默认值限制，必须将要允许使用服务的用户或组添加到访问控制列表中。

服务器服务认证服务提供权限帐户证书（RAC），例如 Web 服务、邮件服务器和文件管理服务器之类的服务可使用它们访问受 RMS 保护的内容，例如：文件服务器，用户可在其中上传不受保护的文档，但下载的文档将自动具有根据内容类型的权限策略应用的 RMS 保护。

（2）使用 SSL 确保 AD RMS 服务的访问安全

建议启用安全套接字层（SSL）并要求对每个 RMS Web 服务文件进行 128 位加密。这些文件具有.asmx 文件扩展名，位于 Licensing、Certification 和 Admin 虚拟目录中。SSL 要求服务器具有为网站安装的有效 SSL 证书。如果用户对 RMS 安装的_wmcs 文件夹启用 SSL，则子文件夹和文件将继承该设置。

（3）设置强私钥密码

私钥密码用于生成私钥并将其安全存储在 AD RMS 配置数据库中。建议使用强密码以确保最大的安全性。注意，如果丢失或忘记了私钥密码，且 AD RMS 服务器意外脱机，则必须对所有 AD RMS 文档进行解密，重建 AD RMS 环境，然后使用新的私钥再次对所有内容进行加密。